CA Identity Manager

Versionshinweise

r12



CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden CA-Produkte:

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center (SCC)
- CA Audit
- eTrust® Directory, auch bezeichnet als CA Directory

Kontakt zum Kundendienst

Für technische Unterstützung online sowie eine vollständige Liste der Standorte, der Servicezeiten und der Telefonnummern wenden Sie sich an den Kundendienst unter http://www.ca.com/worldwide.

Inhalt

Kapitel 3: Änderungen an vorhandenen Funktionen 33

Kapitel 4: Systemvoraussetzungen 37

Kapitel 5: Hinweise zur Installation 39

Kapitel 6: Bekannte Probleme 47

Kapitel 7: Dokumentation 73

Kapitel 1: Willkommen

Diese Datei enthält Hinweise zur Produktinstallation, zur Betriebssystemunterstützung und zu bekannten Problemen sowie Informationen darüber, wie der technische Support von CA kontaktiert werden kann.

Kapitel 2: Neue Funktionen

Dieses Kapitel enthält folgende Themen:

Unterstützte Plattformen und Versionen

In Identity Manager r12 werden zusätzliche Anwendungsserver-Versionen, Verzeichnisse und Datenbanken unterstützt.

Hinweis: Eine vollständige Liste unterstützter Plattformen und Versionen finden Sie in der Identity Manager-Support-Matrix auf der Identity Manager-Support-Site http://ca.com/support.

Die Architektur von Identity Manager

Die Architektur von Identity Manager r12 wurde gegenüber älteren Versionen an folgenden Stellen geändert:

- **Eingebetteter Bereitstellungsserver und Bereitstellungs-Manager**

  Der Bereitstellungsserver ist der Server, der zusätzliche, einem Identity Manager-Benutzer zugewiesene Konten verwaltet. Wenn einem Identity Manager-Benutzer eine Bereitstellungsrolle zugewiesen wurde, erstellt der Bereitstellungsserver an Endpunkten Konten, die die Anforderungen der Rolle erfüllen. Wenn Sie beispielsweise eine Bereitstellungsrolle zuweisen, die eine Vorlage für ein Exchange-Konto enthält, weist der Bereitstellungsserver dem Benutzer ein Exchange-Konto zu.

  Der Bereitstellungs-Manager ist die Benutzeroberfläche zur Verwaltung von Endpunkttypen wie Exchange oder Oracle und von Endpunkten, z.B. von spezifischen Systemen, auf denen Exchange installiert ist. Diese Benutzeroberfläche hieß früher eTrust Admin Manager. Der Bereitstellungs-Manager enthält neue Funktionen wie das Durchsuchen und Korrelieren von Konten. Diese zusätzlichen Funktionen stehen auch in der Identity Manager-Benutzerkonsole zur Verfügung, wo sie leichter zugänglich sind.

  Ältere Versionen von Identity Manager benötigten eTrust Admin für die Bereitstellung.

  Hinweis: Bereitstellungsserver und Bereitstellungs-Manager sind optionale Komponenten.

- **Integration von Identity Manager und SiteMinder**

  Für die Installation von Identity Manager wird SiteMinder nicht mehr vorausgesetzt. Eine Integration mit SiteMinder ist als Option möglich. Dadurch werden erweiterte Funktionen wie SiteMinder-Authentifizierung und erweiterte Kennwortrichtlinien bereitgestellt.

  Ältere Versionen von Identity Manager benötigten SiteMinder für folgende Funktionen:

  – Authentifizierung
  – Speichern von Rollen- und Aufgabeninformationen (im Richtlinienspeicher)
  – Verbindung zu einem Benutzerspeicher
  – Kennwortrichtlinien

  In Identity Manager ist diese Funktion integriert.

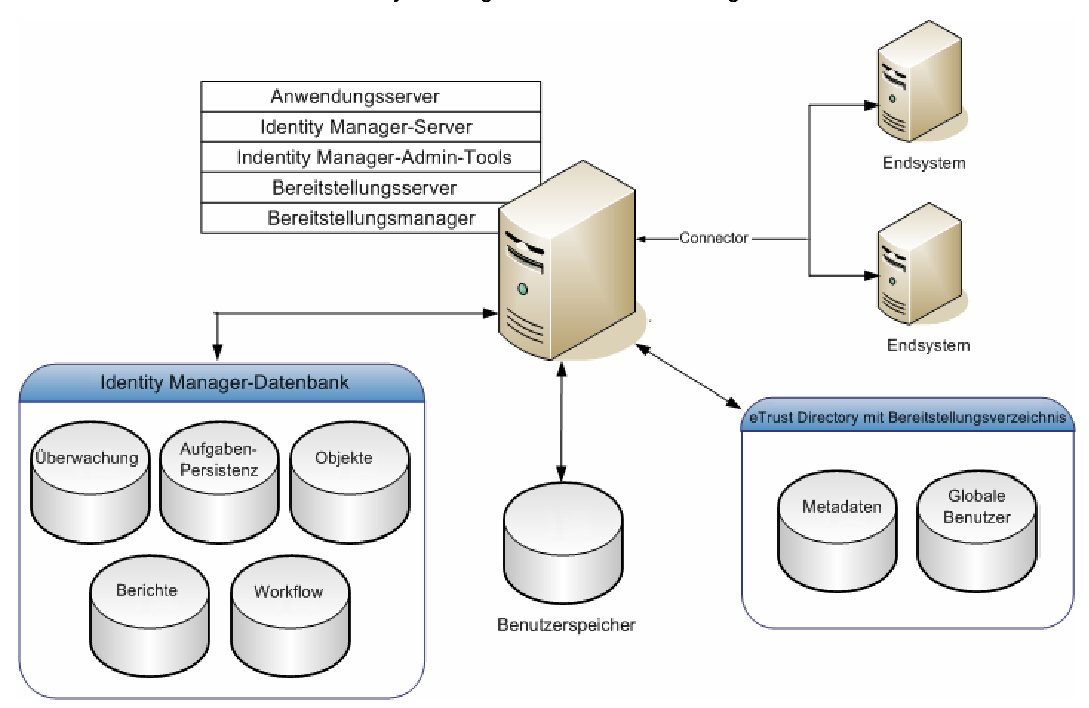
  Hinweis: Durch eine Integration mit SiteMinder werden erweiterte Funktionen wie SiteMinder-Authentifizierung und erweiterte Kennwortrichtlinien bereitgestellt.

- **Objektspeicher**

  In Identity Manager r12 werden jetzt Rollen- und Aufgabeninformationen in einem neuen Objektspeicher gespeichert. Der Objektspeicher ist eine relationale Datenbank, die von Identity Manager automatisch zur Laufzeit konfiguriert wird.

Die folgende Abbildung veranschaulicht eine Implementierung von Identity Manager einschließlich Bereitstellung.

Hinweis: Das Bereitstellungsverzeichnis, in dem für die Bereitstellung und für Informationen zu globalen Benutzern erforderliche Daten gespeichert werden, muss in eTrust Directory installiert werden. Dies ist eine Vorbedingung für die Installation von Identity Manager mit Bereitstellung.



Verbesserung der Installation

Alle für die Server-Installation von Identity Manager erforderlichen Komponenten werden von einem einzigen Installationsprogramm installiert. Dazu gehören Komponenten für die Bereitstellung und Erweiterungen für einen SiteMinder-Richtlinienserver.

Das Installationsprogramm von Identity Manager stellt den Bereitstellungsserver, das Bereitstellungsverzeichnis und den Bereitstellungs-Manager von Identity Manager bereit. Es konfiguriert auch Verbindungen zu den Datenbanken, in denen Objektdaten und Daten zu Workflow, Persistenz, Berichten und Überwachung gespeichert werden.

Die Installation von Identity Manager wurde wie folgt geändert:

- Identity Manager benötigt nicht mehr SiteMinder für die Authentifizierung.
- Die Aufgaben-Persistenz ist nicht mehr optional und wird bei der Installation aktiviert.
- Für jede von Identity Manager verwendete Datenbank wird automatisch ein Datenbankschema erweitert.
- Die Verwaltung wird jetzt an folgenden Positionen installiert:
  - **Windows:** C:\Programme\CA\IAM Suite\Identity Manager\tools
  - **UNIX:** *HOME*/CA/IAM_Suite/Identity_Manager/tools
- Nach der Installation müssen keine Skripts mehr ausgeführt werden.

Verbesserung der Berichte

Identity Manager-Berichte ermöglichen die Anzeige des aktuellen Status einer Identity Manager-Umgebung. Anhand dieser Informationen können Sie die Konformität mit internen Geschäftsrichtlinien oder externen Vorschriften gewährleisten.

Identity Manager r12 enthält folgende Verbesserungen für Berichte:

- **Integration mit dem IAM-Berichtsserver**

  Identity Manager r12 verwendet Business Objects Enterprise XI zum Erstellen, Verwalten und Anzeigen von Berichten aus der Berichtsdatenbank. Identity Manager stellt eine Laufzeitversion von Business Objects bereit. Daher ist keine zusätzliche Lizenz erforderlich.

- **Neue Admin-Aufgaben für den Export von Daten in die Berichtsdatenbank**

  Identity Manager enthält neue Standardaufgaben, mit denen Daten aus Identity Manager in die Berichtsdatenbank exportiert werden können. Bei jedem Export von Daten in die Berichtsdatenbank wird ein *Snapshot*, eine Darstellung des aktuellen Zustands von durch den Benutzer spezifizierten Objekten in einer Identity Manager-Umgebung, erstellt .

  Mithilfe der Standardaufgaben können Sie Snapshot-Definitionen erstellen und einen Snapshot erstellen, von dem ein Bericht generiert werden kann.

- **Zusätzliche vordefinierte Berichte**

  Identity Manager enthält die folgenden vordefinierten Berichte, die Sie direkt verwenden oder an Ihre Geschäftsanforderungen anpassen können:

  – **Endpunktkonten**

    Liste von Konten mit Name, Eigentümer und Erstellungszeit des Kontos für jeden Endpunkt, nach Endpunkttyp sortiert.

  – **Sonderkonten**

    Liste der Sonderkonten wie verwaiste Konten oder Systemkonten.

  – **Sonderkontentrends**

    Sonderkontentrends nach Sonderkontentyp als Diagramm dargestellt.

  – **Verwaiste Konten**

    Liste der Konten, die keinem Benutzer zugewiesen sind. Verwaiste Konten werden mit Name, Eigentümer und Erstellungszeit des Kontos für jeden Endpunkt aufgeführt und nach Endpunkttyp sortiert.

  – **Richtlinien**

    Liste von Richtlinien einschließlich Richtlinienbedingungen und Aktionen beim Übernehmen oder Entfernen.

  – **Rollenadministratoren**

    Liste der Rollenadministratoren

  – **Rollenmitglieder**

    Liste der Rollenmitglieder.

  – **Rolleneigentümer**

    Liste der Rolleneigentümer

  – **Rollen**

    Liste der Rollen und ihrer Beschreibungen.

  – **Snapshots**

    Liste aller vorhanden Snapshots in der Berichtsdatenbank.

– **Aufgabenrollen**

  Liste der Aufgaben mit Beschreibung, Kategorie und Typ. Für jede Aufgabe werden alle zugewiesenen Rollen angegeben.

– **Benutzerkonten**

  Liste der Konten nach Benutzer. Alle Konten werden mit Kontoname, Kontoattributen und Endpunkt aufgeführt und nach Endpunkt sortiert.

– **Sync-Status von Benutzerrichtlinien**

  Liste der Benutzer einschließlich Richtlinien, die derzeit zugewiesen sind, und Richtlinien, die neu zugewiesen werden müssen.

– **Benutzerprofil**

  Liste der Benutzer mit allen verfügbaren Informationen.

– **Benutzerberechtigungen**

  Liste der Benutzer und der zugeordneten Konten, Rollen und Gruppen.

Verbindungsverwaltung

Die Verbindungsverwaltung wird zum Konfigurieren der Verbindungsdetails für den Datenbankserver in Identity Manager verwendet. Wenn von Identity Manager eine Verbindung mit dem Datenbankserver hergestellt werden muss, werden die Verbindungsdetails verwendet, um die Verbindung mit dem Datenbankserver herzustellen. Die Verbindungsverwaltung ermöglicht das Erstellen mehrerer Verbindungen mit unterschiedlichen Datenbankservern unter einem Verbindungstyp. Für jeden Verbindungstyp können Sie eine Standardverbindung angeben. Über die Management-Konsole müssen Sie einen primären Verbindungstyp für Identity Manager konfigurieren.

Verbesserungen bei der Bereitstellung

In dieser Version können auf der Identity Manager-Benutzerkonsole zusätzliche Aktionen durchgeführt werden. Einige dieser Funktionen waren auch vorher in eTrust Admin Manager verfügbar. Sie können die Benutzerkonsole für folgende Aufgaben verwenden:

- Durchsuchen und Korrelieren von Konten an Endpunkten
- Korrelieren von verwaisten und Systemkonten mit einem Identity Manager-Benutzer
- Überwachen von Bereitstellungsaktionen, z.B. einer Zuweisung einer Bereitstellungsrolle an einen globalen Benutzer

In dieser Version sind zusätzlich folgende Komponenten enthalten:

- Connector Xpress, ein grafisches Tool zum Erstellen von benutzerdefinierten Connectors
- Unterstützung für Dynamic Connector (JNDI und JDBC) zur Verwendung mit von Connector Xpress generierten XML-Metadaten
- Java Connector Server, ein Server, der Anforderungen von Java-Connectors behandelt
- Funktionen für hohe Verfügbarkeit für den C++ Connector Server, bisher als Super Agent bezeichnet.
- Neue Java Connectors für Kerberos zur Verwaltung von Kerberos-Prinzipalen und Kerberos-Kennwortrichtlinien auf Solaris-Servern.
- Neue Java-Connectors für SAP (mit CUA-Support)
- Neue Java-Connectors für Oracle, MS-SQL und 0S/400 für den Java Connector-Server.

  Diese drei Connectors ersetzen die Beispieloptionen, die nicht mehr unterstützt werden.
- Der Bereitstellungs-Manager wurde erweitert und bietet jetzt eine generische Benutzeroberfläche für dynamische JDBC- und JNDI-Endpunkttypen, die mit Connector Xpress erstellt wurden.

DYN GUI

Die DYN GUI im Bereitstellungs-Manager wurde erweitert und bietet nun einen verbesserten Satz an Funktionen, mit denen beliebige Endpunktobjekte mit einem einzigen Bereitstellungs-Manager-Plugin bearbeitet werden können.

Wenn z. B. ein Feld in Connector Xpress abgebildet wird, wird ein Element in den Metadaten platziert, das dieses Feld darstellt. Jedes Mal, wenn ein Objekt in diesem Connector untersucht wird, verwendet die DYN GUI die Metadaten, um die entsprechenden Felder anzuzeigen.

Mit den Änderungen in dieser Version werden die Möglichkeiten der DYN GUI durch einen erweiterten Funktionssatz ausgebaut, zukünftige Funktionserweiterungen vereinfacht und die Anzeige für den Benutzer verbessert.

Lotus Notes/Domino-Connector als Technologievorschau freigegeben

Für die r12-Version von Identity Manager wurde der Java-basierte LND-Connector nur als Technologievorschau freigegeben.

Dieser Connector ist **nicht** für Produktionsumgebungen zertifiziert. Der vollständig zertifizierte Connector wird in einem CR (Cumulative Release) verfügbar sein. Wenden Sie sich für weitere Informationen an die für Ihr CA-Konto zuständige Person.

Hinweis: Installieren Sie den C++ LND-Connector und den Java-LND-Connector nicht in derselben Identity Manager-Umgebung.

Verbesserte Statusberichterstellung

Identity Manager r12 enthält mehrere Funktionen, mit denen der Status von Identity Manager-Aufgaben angezeigt werden kann.

Verbesserungen beim Anzeigen von gesendeten Aufgaben

Identity Manager r12 umfasst die Registerkarte "Gesendete Aufgaben anzeigen", auf der der Status einer Aufgabe, die Abhängigkeiten einer Aufgabe von anderen Aufgaben und der Workflow angezeigt werden.

In Identity Manager r12 wurden an der Registerkarte "Gesendete Aufgaben anzeigen" Folgendes verbessert:

- Auf der Registerkarte "Gesendete Aufgaben anzeigen" werden weitere Einzelheiten zu Aufgaben und den mit ihnen verknüpften Ereignissen angezeigt.
- Ausstehende Aufgaben können abgebrochen und fehlgeschlagene Aufgaben können von der Registerkarte "Gesendete Aufgaben anzeigen" aus erneut gesendet oder abgelehnt werden.
- Die Registerkarte "Gesendete Aufgaben anzeigen" kann jetzt konfiguriert werden.

Die Aufgabe "Benutzeraktivität anzeigen"

Bei der Benutzeraktivität handelt es sich um den Aufgabenverlauf eines bestimmten Benutzers. Administratoren können die Aufgabe "Benutzeraktivität anzeigen" verwenden, um die folgenden Benutzerinformationen zu verfolgen:

- Aufgaben, die für den Benutzer durchgeführt wurden

- Aufgaben, die vom Benutzer durchgeführt wurden
- Workflow-Genehmigung, die vom Benutzer durchgeführt wurden

So zeigen Sie die Benutzeraktivität an:

1. Klicken Sie auf die Optionen "Benutzer", "Benutzer verwalten", "Benutzeraktivität anzeigen".

   Das Fenster "Benutzer auswählen" wird angezeigt.

2. Suchen Sie nach einem Benutzer und klicken Sie auf "Auswählen".

   Das Fenster "Benutzeraktivität anzeigen" wird angezeigt.

   Weitere Informationen zur angezeigten Benutzeraktivität finden Sie in der *Online-Hilfe zur Benutzerkonsole*.

Registerkarte "Benutzerverlauf"

Mit der Registerkarte "Benutzerverlauf" können Sie Aufgaben anzeigen, die sich auf Benutzer beziehen. Diese Registerkarte kann einer Aufgabe "Benutzer ändern" oder "Benutzer anzeigen" hinzugefügt werden.

Hinweis: Diese Registerkarte ist in der Standardaufgabe "Benutzeraktivität anzeigen" enthalten.

Die auf dieser Registerkarte angezeigten Aufgabendetails können auch auf der Registerkarte "Übermittelte Aufgaben anzeigen" angezeigt werden.

Verbesserungen des Workflows

In Identity Manager r12 wurden Workflow-Funktionen verbessert, wodurch das Erstellen eines Workflows vereinfacht wird und neue Funktionen hinzugefügt wurden. Diese Verbesserungen werden in den folgenden Abschnitten erläutert.

Workflow-Prozessvorlagen

Mit Workflow-Prozessvorlagen kann die Steuerung der Workflows vollständig von der Identity Manager-Benutzerkonsole aus erstellt und verwaltet werden. Diese generischen Prozessvorlagen können für die Steuerung der meisten Identity Manager-Aufgaben konfiguriert werden.

Die neuen Prozessvorlagen ermöglichen die Workflowkontrolle sowohl auf Aufgaben- als auch auf Ereignisebene, eine einfachere Resolver-Konfiguration für Genehmiger und Genehmigungsprozesse in mehreren Schritten.

Die Liste der Genehmiger kann auch abhängig von den Attributen der zu genehmigenden Aufgabe oder des Ereignisses dynamisch zur Laufzeit bestimmt werden.

Workflow auf Aufgabenebene

Ein Workflow-Prozess kann sowohl mit Aufgaben als auch mit Ereignissen verknüpft werden. Dies bedeutet, dass die Teilnehmer eine ganze Identity Manager-Aufgabe oder ein spezielles Ereignis in einer Aufgabe genehmigen oder ablehnen können.

Der Workflow auf Aufgabenebene ermöglicht es den Teilnehmern, alle Ereignisse zu überprüfen, bevor sie entscheiden, ob eine Anforderung genehmigt oder abgelehnt wird. Wenn ein Workflow-Prozess mit einem bestimmten Ereignis in einer Aufgabe verbunden ist, kann der Genehmiger den gesamten Aufgabenkontext, in dem eine Anforderung gestellt wird, nicht sehen.

Schaltflächen für Workflow-Aktionen

Als Ergänzung oder Ersatz für die Standardschaltflächen zum Genehmigen oder Ablehnen können zu Workflow-Genehmigungsaufgaben neue Schaltflächen hinzugefügt werden. Ein Beispiel für diese Funktion wird in den Online-Anfrage-Aufgaben veranschaulicht.

Online-Anfragen und Verlauf

An der Benutzerkonsole können Benutzer Änderungen an ihren eigenen Konten und Administratoren Änderungen an Benutzerkonten anfordern. Diese Aufgaben lösen eine Workflow-Prozessvorlage aus, die bis zu drei Genehmiger benötigt: einen Berater, der die Anforderung kommentiert, einen Geschäftsbenutzer zur Genehmigung der Anforderung und einen Fachmann, der die Anforderung umsetzt.

Die Online-Anfrage-Aufgaben beinhalten ein neues Verlaufssteuerelement, mit dem Genehmiger der Aufgabe in den verschiedenen Phasen der Durchführung Anmerkungen oder Kommentare hinzufügen können.

Aufgabenpläne

Mit Hilfe von Ablaufplänen können Sie die Ausführung einer Aufgabe zu einem späteren Zeitpunkt automatisieren. Wenn Sie eine mit einem Workflow-Prozess verknüpfte Aufgabe planen, führt Identity Manager alle Aufgaben wie im Prozess definiert aus. Der Status der geplanten Aufgabe wird auf der Seite "Gesendete Aufgaben anzeigen" angezeigt.

Eine geplante Aufgabe, die noch nicht von Identity Manager ausgeführt wurde, kann über die Seite "Übermittelte Aufgaben anzeigen" neu geplant bzw. verworfen werden.

In Identity Manager wird der Scheduler als spezielle Registerkarte bereitgestellt. Um auf den Scheduler zugreifen zu können, müssen Sie eine Aufgabe über die Registerkarte "Ablaufplan" konfigurieren.

Verbesserungen der Benutzerkonsole

Identity Manager r12 bietet jetzt durch mehrere Verbesserungen Unterstützung für neue Funktionen und eine vereinfachte Bedienung. Diese Verbesserungen werden in den folgenden Abschnitten dargestellt.

Benutzerdefinierte Hilfe

In Identity Manager können Sie eine eigene benutzerdefinierte Hilfe für Aufgaben und Registerkarten erstellen, die Sie in der Benutzerkonsole angepasst haben. Sie können ein kontextsensitives Hilfesystem mit eigenen HTML-Hilfeseiten oder Wiki-Seiten erstellen und die Hilfe-Links zum Zugriff auf die benutzerdefinierte Hilfe in der Identity Manager-Benutzerkonsole umleiten.

Mithilfe dieser Funktionen können Sie auch die (englische) Standard-Hilfe in eine andere Sprache übersetzen.

Geschachtelte Aufgaben

Als geschachtelte Aufgabe wird eine Admin-Aufgabe bezeichnet, die über die Registerkarte "Profil" einer anderen Aufgabe geöffnet werden kann. Benutzer der ersten Aufgabe öffnen die geschachtelte Aufgabe durch Klicken auf eine Verknüpfung oder Schaltfläche. Sie können beispielsweise für die Aufgabe "Benutzer ändern" eine Schaltfläche mit der Bezeichnung "Benutzer löschen" hinzufügen. Ist ein Benutzerkonto nicht mehr gültig, kann ein Administrator es über die Schaltfläche "Benutzer löschen" entfernen, ohne zum Navigationsbereich zurückkehren und eine neue Aufgabe auswählen zu müssen.

Registerkartensteuerungen

Registerkartensteuerungen bestimmen, wie die Registerkarten in einer Aufgabe angezeigt werden. Sie wählen einen der folgenden Registerkartensteuerungen aus:

- **Standard-Registerkartensteuerung**

  Zeigt die Registerkarten für die Aufgabe als separate Registerkarten an. Die Benutzer können die Registerkarten in der Aufgabe in beliebiger Reihenfolge verwenden.

  Hierbei handelt es sich um die standardmäßige Registerkartensteuerung.



- **Assistenten-Registerkartensteuerung**

  Zeigt die Registerkarten in einer Aufgabe als Assistenten an. Administratoren verwenden jede Registerkarte nacheinander.



- **Sequenzielle Registerkartensteuerung**

  Zeigt eine Registerkarte an, die jeweils als eine einzelne Seite angezeigt wird. Die Benutzer schließen eine Registerkarte ab und klicken dann auf eine benutzerdefinierte Schaltfläche oder einen Link, um zur nächsten Registerkarte zu gelangen.

  Die Reihenfolge der Registerkarten und die Schaltflächen sowie Links, die angezeigt werden, werden programmatisch von einem JavaScript festgelegt. Das JavaScript wird beim Konfigurieren der sequenziellen Registerkartensteuerung geschrieben.

  Im benutzerdefinierten JavaScript können Sie die Darstellung und die Reihenfolge der Registerkarten basierend auf der Benutzereingabe angeben. Wenn ein Benutzer beispielsweise auf der ersten Registerkarte eine Option auswählt, zeigt Identity Manager eine Seite an. Wählt der Benutzer eine andere Option aus, so wird eine andere Seite angezeigt.



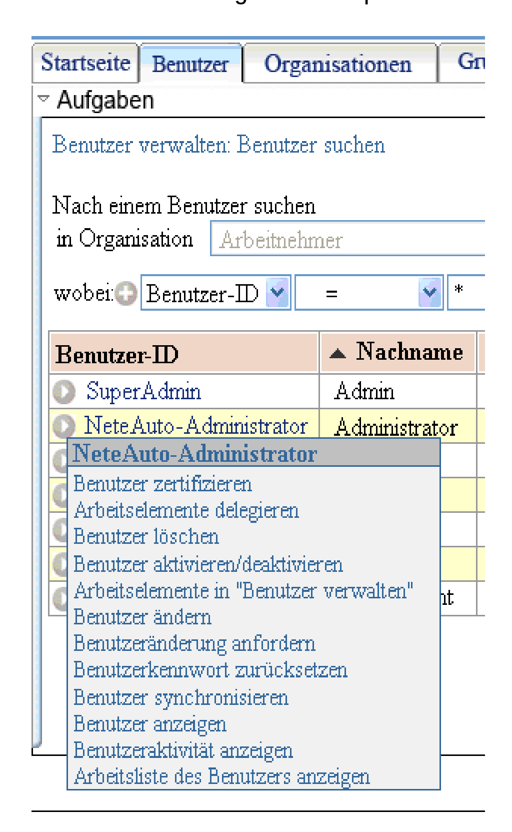
Aufgabenlisten

Identity Manager r12 enthält die folgenden neuen Standardaufgaben, mit denen nach einem zu verwaltenden Objekt gesucht werden kann:

- Benutzer verwalten
- Gruppen verwalten
- Organisationen verwalten
- Admin-Rollen verwalten
- Admin-Aufgaben verwalten
- Zugriffsrollen verwalten
- Zugriffsaufgaben verwalten

Nach Auswählen des Objekts können Sie eine Liste mit Aufgaben anzeigen, die Sie zum Verwalten dieses Projekts verwenden können.

Wenn Sie beispielsweise einen Benutzer mithilfe dieser Methode ändern möchten, wählen Sie zunächst die Kategorie "Benutzer" und dann die Aufgabe "Benutzer verwalten" aus. Sie wählen den Benutzer aus, den Sie verwalten möchten. Klicken Sie in den Suchergebnissen auf ein Symbol, um eine Liste mit Aufgaben anzuzeigen, die Sie zum Verwalten des ausgewählten Benutzers verwenden können. In dieser Liste können Sie die Aufgabe "Benutzer ändern" bzw. eine beliebige andere passende Aufgabe auswählen.



Sie können Aufgabenlisten auch in anderen als den Verwaltungsaufgaben konfigurieren. Sie können eine Aufgabenliste beispielsweise zur Registerkarte "Mitgliedschaft" hinzufügen. In diesem Fall ist für jedes Mitglied eine Aufgabenliste verfügbar, das auf der Registerkarte "Mitgliedschaft" angezeigt wird.

Verbesserungen der Registerkarte "Profil"

Die Registerkarte "Profil" in Identity Manager r12 bietet einige neue Konfigurationseinstellungen zur Unterstützung von neuen Funktionen. Diese neuen Einstellungen werden in den folgenden Abschnitten erläutert.

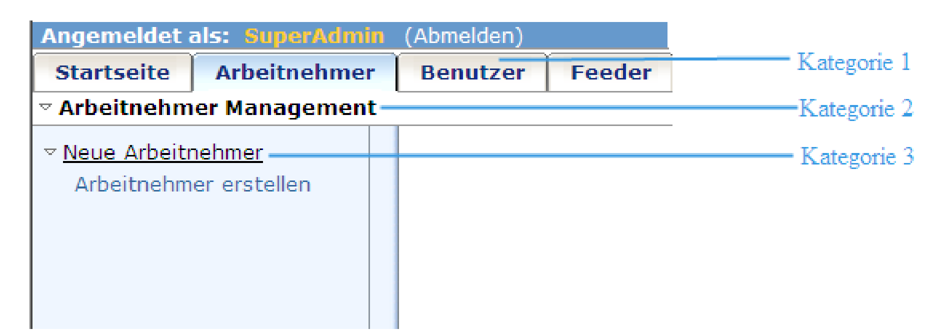
Aufgabenkategorien

Aufgabenkategorien ermöglichen die Organisation von Aufgaben, um sie in der Benutzerkonsole einfacher auffindbar zu machen.

Sie können drei Aufgabenkategorien angeben:

- Bei Kategorie 1 handelt es sich um die Kategorie der höchsten Ebene für Aufgaben. Diese Kategorien werden oben in der Benutzerkonsole als Registerkarten angezeigt.
- Bei Kategorie 2 handelt es sich um die Kategorie der zweiten Ebene. Diese Kategorie ermöglicht die Gruppierung verwandter Aufgaben in einer Kategorie der höchsten Ebene. Falls Sie keine Kategorie der zweiten Ebene angeben, handelt es sich bei der Standardkategorie um "Aufgaben".
- Kategorie 3 enthält die Aufgaben, die Administratoren verwenden. Wenn Administratoren in der Benutzerkonsole auf den Namen "Kategorie 3" klicken, wird eine Liste mit Aufgaben dieser Kategorie angezeigt.

Innerhalb jeder Kategorie können Sie die Reihenfolge steuern, in welcher die Elemente dieser Kategorie angezeigt werden, indem Sie eine Kategorie-Reihenfolge angeben. In der folgenden Abbildung weist die Registerkarte "Arbeitnehmer" beispielsweise die Kategorie-Reihenfolge 3 auf.



Hinweis: Wenn eine Kategorie mehrere Aufgaben enthält, muss die Kategorie-Reihenfolge, die im Profil einer jeden Aufgabe angegeben ist, gleich sein. Wenn die Kategorie-Reihenfolge unterschiedlich ist, werden mehrere Instanzen dieser Kategorieregisterkarte angezeigt. Die Kategorie "Arbeitnehmer" weist beispielsweise zwei Aufgaben auf: "Arbeitnehmer erstellen" und "Arbeitnehmer ändern". Wenn die Kategorie-Reihenfolge in der Aufgabe "Arbeitnehmer erstellen" 3 und die Kategorie-Reihenfolge in der Aufgabe "Arbeitnehmer ändern" 6 ist, wird die Kategorie "Arbeitnehmer" als zwei Registerkarten angezeigt.

Aufgabenpriorität

In Identity Manager r12 können Sie jetzt durch eine Aufgabenpriorität festlegen, dass Identity Manager zeitkritische Aufgaben zuerst durchführt.

Die Priorität einer Aufgabe kann auf der Registerkarte "Profil" der Aufgabe auf "Hoch", "Mittel" oder "Niedrig" gesetzt werden. Die Standardpriorität ist "Mittel".

Hinweis: Sie können die Aufgabe "Übermittelte Aufgaben anzeigen" verwenden, um nach Aufgaben mit einer bestimmten Priorität zu suchen und dann deren Status anzuzeigen.

Benutzerdefinierte Daten für Auswahlfelder

Die Aufgabenfenster in Identity Manager weisen Felder auf, über die die Benutzer einen Wert auswählen können. Zu diesen Feldern zählen die folgenden:

- Mehrfachauswahl-Kontrollkästchen
- Dropdown
- Dropdown-Kombinationsfeld
- Mehrfachauswahl
- Optionsauswahl
- Kombinationsfeld für Optionsauswahl
- Optionsfeld mit Einfach-Auswahl
- Einfachauswahl

Sie können benutzerdefinierte Daten angeben, die Sie zum Füllen von Feldern in XML-Dateien verwenden möchten. Sie können beispielsweise die XML-Dateien "Auswahlfelddaten" verwenden, um Optionen für das Dropdown-Feld "Stadt" oder "Bundesstaat" auf der Registerkarte "Profil" für die Aufgabe "Benutzer erstellen" zu füllen.

Sie können die XML-Datei "Auswahlfelddaten" auch verwenden, um eine Abhängigkeit zwischen zwei Feldern in einem Aufgabenfenster zu konfigurieren. Die Optionen im Feld "Stadt" können beispielsweise von der Option abhängen, die ein Benutzer für das Feld "Bundesstaat" auswählt.

Das Steuerelement "Datumsauswahl"

Die Identity Manager-Benutzerkonsole enthält jetzt eine Formatvorlage "Datumsauswahl", die Felder auf eine Registerkarte "Profil" angewendet werden kann, die Datumsangaben aufnehmen und anzeigen.

Wenn die Formatvorlage "Datumsauswahl" angewendet wird, wird neben dem Datumsfeld ein Kalendersymbol eingeblendet. Benutzer können durch Klicken auf das Kalendersymbol ein Kalendersteuerelement anzeigen, in dem sie das gewünschte Datum auswählen können.

Binäre und grafische Steuerelemente

Sie können in Identity Manager jetzt das Anzeigen eines Bildes oder eines binären Attributs in einem Profil konfigurieren. Sie können das Fenster eines Benutzerprofils beispielsweise so konfigurieren, dass ein Digitalfoto des betreffenden Benutzers angezeigt wird, oder Sie können dem Profilfenster ein Dokument zuordnen.

Hinweise: Diese Funktion wird nur für LDAP-Benutzerspeicher unterstützt.

Benutzerdefinierte kundenspezifische Attribute für Rollen

Identity Manager unterstützt benutzerdefinierte kundenspezifische Attribute, mit denen Sie Rollen in Ihrer Organisation effektiv filtern können. Es kann zum Beispiel in Ihrer Unternehmensumgebung die Notwendigkeit bestehen, mehr als eintausend Rollen zu erstellen. Außerdem möchten Sie diese Rollen möglicherweise nach Geschäftseinheiten und geografischen Standorten sortieren. Wenn Sie nach Rollen suchen möchten, die nur für einen bestimmten geografischen Standort gelten, können Sie die kundenspezifisch definierten Attribute verwenden, um diese Rollen in Ihrer Organisation herauszufiltern.

Sie können kundenspezifische Attribute in den Aufgaben "Erstellen", "Ändern" und "Anzeigen" mit folgenden Rollen verwenden:

- Zugriffsrollen
- Admin-Rollen

Sie müssen folgende Schritte durchführen, um kundenspezifische Attribute zu Admin-Aufgaben und Suchfenstern hinzuzufügen.

1. Fügen Sie kundenspezifische Attribute beliebigen Admin-Aufgaben hinzu, die für die Rollen definiert sind.
2. Konfigurieren Sie die Suchfenster für die Rollen mit kundenspezifischen Attributen.

Bulk Loader

Die Registerkarte "Bulk Loader" wird auf der Benutzerkonsole zum Hochladen von Feeder-Dateien verwendet, die zum gleichzeitigen Bearbeiten einer großen Anzahl an verwalteten Objekten verwendet werden. Sie können 1000 Benutzer in Identity Manager beispielsweise manuell oder mit Hilfe von Bulk Loader erstellen. Der Vorteil der Bulk Loader-Methode liegt darin, dass Sie den Bearbeitungsprozess einer großen Anzahl an verwalteten Objekten mit einer Informationsdatei (Feeder-Datei) automatisieren können. Die Bulk Loader-Aufgabe kannn darüber hinaus einem Workflow-Prozess zugeordnet werden.

Hinweis: Das für den Feeder unterstützte Dateiformat ist CSV, aber Sie können einen benutzerdefinierten Feed für andere Dateiformate erstellen.

Standard-Organisationssuche auf der Grundlage von Benutzern

Zur Vereinfachung der Benutzerkonsole ermöglicht Identity Manager Administratoren, für die Aufgabe "Benutzer erstellen" eine Standardorganisation auf der Grundlage des Benutzers zur erstellen, der versucht, die Aufgabe auszuführen. Wenn ein Benutzer die Aufgabe "Benutzer erstellen" ausführt, wird die Organisation nicht auf der Registerkarte "Benutzerprofil erstellen" angezeigt, sondern als Standard auf Grundlage der Organisation des Benutzers festgelegt.

So konfigurieren Sie eine Standardorganisation auf der Grundlage eines Benutzers

1. Wählen Sie auf der Benutzerkonsole von Identity Manager zunächst die Option "Rollen und Aufgaben" und dann die Optionen "Admin-Aufgaben" und "Admin-Aufgabe ändern" aus.
2. Wählen Sie die Aufgabe "Benutzer erstellen" aus.
3. Klicken Sie auf der Registerkarte "Registerkarten" auf das Pfeil-nach-rechts-Symbol neben "Profil".
4. Klicken Sie auf die Schaltfläche mit der Ellipse (...), um eine Liste der Fenster anzuzeigen, die bearbeitet werden müssen.
5. Wählen Sie das Fenster "Benutzerprofil erstellen" aus, und klicken Sie dann auf "Bearbeiten".
6. Suchen Sie nach "Organisation" und klicken Sie zum Bearbeiten auf das Symbol mit dem Rechtspfeil.

   Hinweis: Dieses Feld ist in einer Umgebung ohne Organisationen nicht vorhanden.
7. Legen Sie für "Formatvorlage" die Option "Ausgeblendet" fest.

8. Geben Sie im Feld "Standard-JavaScript" Folgendes ein:

```
function defaultValue(blthContext)

{

return blthContext.getAdministrator().getOrg(null).getUniqueName();

}
```

9. Klicken Sie auf "Übernehmen".

IPv6-Support

Bei der Konfiguration des Identity Managers können Sie sowohl IPv4- als auch IPv6-Adressen eingeben.

Identity Manager unterstützt IPv6 auf folgenden Betriebssystemen:

- Solaris 8 oder höher
- Windows XP SP1 oder höher
- Windows 2003 oder höher

Jeder Anwendungsserver hat spezifische JDK-Anforderungen:

- Für einen JBoss-Anwendungsserver auf einem Standalone-System unterstützt Identity Manager IPv6 mit JDK1.4.2_13 oder 1.5 (unter Solaris) oder JDK1.5 (unter Windows).
- Es steht kein JDK für einen JBoss-Cluster zur Verfügung, der zum Zeitpunkt der Freigabe von Identity Manager r12 mit IPv6 funktioniert. Sobald ein JDK freigegeben wird, das mit IPv6 funktioniert, wird die Plattform-Support-Matrix aktualisiert.
- Jedoch unterstützt Identity Manager IPv6 mit JDK1.4.2_13 oder 1.5 (unter Solaris) oder JDK1.5 (unter Windows) für JBoss-Cluster, die einen IPv4/IPv6-Stack verwenden.
- WebLogic- und WebSphere-Anwendungsserver beinhalten JDK 1.5, das IPv6-Adressen unterstützt.

Beachten Sie Folgendes, bevor Sie eine Umgebung konfigurieren, die IPv6 unterstützt:

- Damit Identity Manager IPv6-Adressen unterstützen kann, müssen alle Komponenten in der Implementierung von Identity Manager, einschließlich Betriebssystem, JDK, Verzeichnisserver und Datenbanken, ebenfalls IPv6-Adressen unterstützen.
- Wenn Identity Manager mit SiteMinder integriert ist, muss das Webserver-Plugin für den Anwendungsserver ebenfalls IPv6 unterstützen.

- Wenn Sie vom Identity Manager eine Verbindung zu SiteMinder oder zu einer Datenbank über eine JDBC-Verbindung herstellen, geben Sie den Hostnamen und nicht die IP-Adresse an.
- Der IAM-Berichtsserver kann auf einem Dual-Stack-Host installiert werden, der IPv4 und IPv6 unterstützt, aber die Kommunikation mit dem Server muss über IPv4 erfolgen.

  Wenn Sie in der Management-Konsole eine Verbindung zum Berichtserver konfigurieren, muss der Servername im IPv4-Format angegeben werden.

FIPS 140-2

Identity Manager r12 unterstützt FIPS 140-2 *nur* in einer neuen Installation. Außerdem verfügt Identity Manager über ein Kennwort-Tool zur Bereitstellung eines FIPS-Verschlüsselungsschlüssels, der sich im folgenden Verzeichnis befindet:

```
<Installationspfad>\PasswordTool
```

Beachten Sie beim Aktivieren von FIPS 140-2 für eine Identity Manager-Umgebung Folgendes:

- Sobald die FIPS 140-2-Unterstützung für eine Identity Manager-Bereitstellung einmal aktiviert wurde, kann sie nicht mehr deaktiviert werden. Ebenso kann, wenn Sie Identity Manager ohne aktivierte FIPS 140-2-Unterstützung installieren, die Unterstützung zu einem späteren Zeitpunkt nicht mehr hinzugefügt werden.
- Wenn Sie FIPS 140-2 in einer Identity Manager-Bereitstellung aktivieren möchten, die SiteMinder beinhaltet, muss es sich bei der SiteMinder-Version um r12 handeln.

Erweiterte Lokalisierungsunterstützung

Die Identity Manager-Benutzerkonsole und die Online-Hilfe der Benutzerkonsole sind in folgenden Sprachen verfügbar:

- Französisch
- Koreanisch
- Japanisch
- Deutsch

- Chinesisch (Vereinfacht)
- Spanisch
- Italienisch

Hinweis: Informationen zur Verwendung von Identity Manager in einer dieser Sprachen finden Sie im *Konfigurationshandbuch*.

Weitere Informationen:

Installation von lokalisierten Identity Manager-Umgebungen (siehe Seite 41)

Kapitel 3: Änderungen an vorhandenen Funktionen

Dieses Kapitel enthält folgende Themen:

Servlet-Filteragent ist veraltet

Von der Verwendung des Servlet-Filteragenten in Identity Manager r12 wird abgeraten. Wir empfehlen die Verwendung eines Web-Agenten anstelle eines Servlet-Filteragenten. Ein bereits in einer *vorhandenen* Identity Manager-Umgebung bereitgestellter Servlet-Filteragent funktioniert aber und wird weiterhin unterstützt.

Verbesserungen der Management-Konsole

Die Identity Manager-Management-Konsole enthält folgende neue oder geänderte Fenster:

- Seite "Benutzerkonsole": Auf dieser Seite können allgemeine Einstellungen einer Identity Manager-Benutzerkonsole festgelegt werden, z.B. Symbol, Titel, die Authentifizierungsklasse und die Abmeldeseite.

  Hinweis: In Identity Manager wurden Symbol und Titel auf der Seite "Design" konfiguriert. Die Funktionen der Seite "Design" wurden auf die Seite "Benutzerkonsole" übertragen, und die Seite "Design" wurde entfernt.

- Seite "Umgebungen": Auf der Seite "Umgebungen" kann jetzt eine Identity Manager-Umgebung gestartet und angehalten werden. Der Anwendungsserver muss nicht neu gestartet werden, damit Änderungen der Umgebung wirksam werden.

- Seite "Bereitstellung": Die Konfiguration der eingehenden Synchronisierung befindet sich nicht mehr auf dieser Seite. Informationen zur Konfiguration der eingehenden Synchronisierung finden Sie im *Bereitstellungshandbuch*.
- Seite "Aufgaben-Persistenz": Die Aufgaben-Persistenz wird jetzt automatisch bei der Installation konfiguriert. Die Aufgaben-Persistenz muss nicht mehr manuell aktiviert werden. Diese Seite wurde entfernt.

Änderungen der Kennwortrichtlinie

Da neue Installationen von Identity Manager r12 SiteMinder nicht mehr benötigen, wurde die Standard-Funktionalität der Kennwortrichtlinie in einigen Punkten geändert. In Bereitstellungen ohne Integration von SiteMinder ermöglicht Identity Manager das Erstellen von Basis-Kennwortrichtlinien zur Verwaltung von Benutzerkennwörtern, wobei Regeln und Einschränkung im Hinblick auf Ablauf, Zusammensetzung und Verwendung der Kennwörter erzwungen werden.

Wenn Identity Manager in SiteMinder integriert ist, können Sie erweiterte Kennwortrichtlinien erstellen, mit denen Sie die folgenden zusätzlichen Regeln und Einschränkungen definieren können:

- Verzeichnisfilter
- Ablauf des Kennworts:
  - Fehlgeschlagene oder erfolgreiche Anmeldeversuche verfolgen
  - Authentifizierung beim Anmelden
  - Das Kennwort läuft ab, wenn es nicht geändert wird
  - Kennwort-Inaktivität
  - Ungültiges Kennwort
- Mehrere reguläre Ausdrücke
- Beschränkungen für Kennwort:
  - Mindestanzahl von Tagen vor Wiederverwendung
  - Mindestanzahl von Kennwörtern vor Wiederverwendung
  - Prozentualer Unterschied zum letzten Kennwort
  - Bei der Prüfung auf Unterschiede Sequenz ignorieren
  - Profilattribut-Abgleich
  - Wörterbuch-Abgleich

Tool "imrexport" veraltet

Die Funktionen des Tools "imrexport" wurden in die Identity Manager-Benutzerkonsole integriert. Die Aufgabe "Snapshot-Daten erfassen" auf der Registerkarte "Berichte" umfasst jetzt in Identity Manager r12 die Funktionen des Tools "imrexport".

Änderung der z/OS Connectors-Architektur

Die Architektur der z/OS Connectors (CA ACF2, CA Top Secret und RACF) wurde aus Gründen der Systemleistung überarbeitet, weshalb jetzt anstelle des CA DSI-Servers unter z/OS der CA LDAP-Server für z/OS verwendet wird.

Alle Konfigurationsdateioptionen für den Bereitstellungsserver, die mit dem CA LDAP-Server zu tun haben, werden jetzt unter z/OS erfasst und gespeichert, wenn der CA LDAP-Server installiert wird. Auch Informationen über die Mainframe-LDAP-Server-Verbindung werden jetzt über die Endpunktaufgabenansicht des Bereitstellungs-Managers erfasst.

Nicht mehr unterstützte Funktionen

Einige eTrust Admin-Funktionen sind in Identity Manager r12 nicht mehr verfügbar. Die folgende Tabelle zeigt die neuen Funktionen in Identity Manager r12.

eTrust Admin-Funktion	Identity Manager-Funktion
Advanced Workflow	WorkPoint-Workflow
Legacy-Workflow	WorkPoint-Workflow
Selbstverwaltete Webschnittstelle (SAWI)	Self-Service in Identity Manager
Selbstverwaltete Webschnittstelle (DAWI)	Delegierte Identity Manager-Verwaltung
mit IA Manager	Self-Service-Aufgaben in Identity Manager und delegierte Verwaltung
eTrust Admin-Berichte etaReport	Identity Manager-Berichte
PeopleSoft Feed-Option	Bulk Loader
Universelle Feed-Option	Bulk Loader
SAP-Option (C++-Version)	SAP Connector (Java-Version)
MS SQL-Option (C++-Version)	MS Connector (Java-Version)

eTrust Admin-Funktion	Identity Manager-Funktion
Oracle-Option (C++-Version)	Oracle Connector (Java-Version)
OS/400-Option	OS/400 Connector (Java-Version)
CleverPath Portal-Option	Kein Ersatz

Hinweis: Vorhandene Versionen (verfügbar mit eTrust Admin 8.1 SP2) der PeopleSoft Feed-Option und der Universal Feed-Option funktionieren weiterhin mit Identity Manager r12.

Kapitel 4: Systemvoraussetzungen

Es folgen die Mindest-Hardwarevoraussetzungen für ein System, auf dem der Identity Manager-Server gehostet wird:

- CPU: Single oder Dual-Prozessor, Intel Pentium III (oder kompatibel) 700-900 MHz, oder Sparc Workstation 440 MHz
- Arbeitsspeicher: 2 GB
- Erforderlicher freier Speicherplatz: 1 GB

Hinweis: Bei diesen Hardwarevoraussetzungen wurden bereits die Anforderungen des Anwendungsservers berücksichtigt, der auf dem System zusammen mit Identity Manager-Server installiert werden muss.

Kapitel 5: Hinweise zur Installation

Dieses Kapitel enthält folgende Themen:

Support-Matrix-Speicherort

Eine vollständige Liste der unterstützten Softwareversionen finden Sie in der Identity Manager-Support-Matrix.

So finden Sie die Support-Matrix

1. Melden Sie sich unter support.ca.com an.
2. Klicken Sie auf "Support By Product or Solution" (Support nach Produkt oder Lösung).
3. Wählen Sie im Bereich "Select a Product or Solution page" (Produkt- und Lösungsseite wählen) aus der Produktauswahlliste "CA Identity Manager".

   Die CA Identity Manager-Produktseite wird geöffnet.
4. Blättern Sie nach unten bis "Recommend Readings" (Leseempfehlung).
5. Klicken Sie auf "CA Identity Manager Informational Documentation Index" (CA Identity Manager - Informationsdokumentationsindex).

Auf der Seite werden Plattform-Support-Matrizen für unterstützte Versionen von Identity Manager angezeigt.

Solaris-Patches erforderlich

Laden Sie vor der Installation von Bereitstellungen unter Solaris 9 oder 10 Patches herunter und installieren Sie sie:

So laden Sie Sun Studio 10-Patches für SDK herunter

1. Gehen Sie zu folgender URL:
   http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html
2. Laden Sie das Patch 117830 herunter und installieren Sie es.

   Hinweis: Sun Studio 11 erfordert keine Patches.

So laden Sie Solaris 9-Patches für alle Komponenten herunter

1. Gehen Sie zu folgender URL:

   http://search.sun.com/search/onesearch/index.jsp
2. Laden Sie die Datei 9_recommended.zip herunter und installieren Sie sie.

Umgebungsvariable für SiteMinder-Integration benötigt

Wenn Sie Identity Manager auf einem Solaris-System installieren und die Integration mit SiteMinder aktivieren, wird Ihnen womöglich folgender Fehler im Anwendungsserverprotokoll angezeigt und Identity Manager startet eventuell nicht mehr:

Fehler "java: fatal: libetpki2.so: Öffnen fehlgeschlagen: Keine solche Datei oder kein solches Verzeichnis"

Dieser Fehler tritt auf, wenn die CALIB-Umgebungsvariable bei der ETPKI-Installation, die eine für SiteMinder erforderliche Verschlüsselungsbibliothek installiert, nicht korrekt hinzugefügt wurde.

Hinweis: ETPKI wird automatisch vom Identity Manager-Installationsprogramm installiert.

Umgehungslösung

Fügen Sie die CALIB-Umgebungsvariable vor dem Start des Identity Manager-Servers folgendermaßen hinzu:

```
bash# export CALIB=/opt/CA/SharedComponents/ETPKI/lib
```

Installation von lokalisierten Identity Manager-Umgebungen

Identity Manager enthält lokalisierte Versionen von der Identity Manager-Benutzerkonsole und der Online-Hilfe für die Benutzerkonsole. Der Großteil der für eine lokalisierte Version benötigten Dateien ist unter folgendem Speicherort installiert:

im_admin_tools_dir\samples\Localization*language*

im_admin_tools_dir

Gibt das Installationsverzeichnis der Verwaltungswerkzeuge von Identity Manager an.

language

Gibt die Sprache an, die Sie verwenden möchten.

Hinweis: Anweisungen zur Installation finden Sie im *Konfigurationshandbuch*.

Es sind allerdings zusätzliche Dateien für den Einsatz einer lokalisierten Version von Identity Manager erforderlich:

- Versionshinweise
- Online-Hilfedateien

  Hinweis: Verwenden Sie nicht die Version der Online-Hilfedateien, die im Verzeichnis *im_admin_tools_dir*\samples\Localization*language* verfügbar sind.

Die gewünschten Dateien stehen im Download mit den lokalisierten Ressourcen für CA Identity Manager r12 zur Verfügung, den Sie auf der CA Support-Website finden.

So installieren Sie die Online-Hilfedateien

1. Laden Sie die ZIP-Datei mit den lokalisierten Ressourcen für CA Identity Manager r12 herunter.
2. Entzippen Sie die Dateien auf einem System, auf das der Anwendungsserver zugreifen kann, auf dem Identity Manager gehostet ist.
3. Kopieren Sie die Datei im_help_*language*.ZIP für die gewünschte Sprache nach *IdentityMinder.ear*\user_console.war\

   IdentityMinder.ear

   Der Ort, an dem die Identity Manager-Anwendung (IdentityManager.ear) auf dem Anwendungsserver bereitgestellt wird.

   Hinweis: Denken Sie daran, eine Sicherungskopie der ursprünglichen Online-Hilfe zu erstellen, bevor Sie sie durch eine lokalisierte Version ersetzen. Die ursprüngliche Online-Hilfe wird von der lokalisierten Version überschrieben.

4. Entzippen Sie die Datei im_help.zip ins Verzeichnis user_console.war.
5. Starten Sie die Identity Manager-Umgebung neu.

   Die lokalisierte Version der Online-Hilfe ist nun verfügbar.

Nicht-ASCII-Zeichen verursacht Installationsfehler auf nicht englischsprachigen Systemen

Während der Installation von Identity Manager extrahiert das Installationsprogramm Dateien in ein Temp-Verzeichnis. Auf einigen lokalisierten Systemen enthält der Standardpfad zum Temp-Verzeichnis Nicht-ASCII-Zeichen. Der Standardpfad zum Temp-Verzeichnis lautet beispielsweise auf spanischen Windows-Systemen:

C:\Documents and Settings\Administrador\Configuración local\Temp

Das Nicht-ASCII-Zeichen sorgt dafür, dass das Installationsprogramm eine leere Übersichtsseite für die Installationsvorbereitungen anzeigt und die Installation anschließend fehlschlägt.

So sorgen Sie dafür, dass die Installation fehlerfrei verläuft

Ändern Sie die Tmp-Umgebungsvariable so, dass sie auf einen Ordner verweist, der ausschließlich ASCII-Zeichen enthält.

Konfigurationsänderungen für SiteMinder "FIPS 140-2 Only Mode" erforderlich

Wenn sich SiteMinder im "FIPS 140-2 Only Mode" befindet, ist ein zusätzlicher Konfigurationsschritt erforderlich.

So konfigurieren Sie Identity Manager, damit es mit SiteMinder im "FIPS 140-2 Only Mode" auf WebLogic oder JBoss funktioniert.

1. Öffnen Sie *IdentityMinder.ear*\policyserver.rar\META-INF\ra.xml.
2. Suchen Sie folgendes Element:

```
<config-property>
<config-property-name>FIPSMode</config-property-name>
<config-property-type>java.lang.String</config-property-type>
<config-property-value>false</config-property-value>
</config-property>
```

3. Setzen Sie im Element <config-property-value> den Wert von "False" auf "True".
4. Starten Sie den Anwendungsserver neu.

So konfigurieren Sie Identity Manager, damit es mit SiteMinder im "FIPS 140-2 Only Mode" auf WebSphere funktioniert.

1. Öffnen Sie die Verwaltungskonsole von WebSphere.
2. Navigieren Sie zu folgendem Verzeichnis:

   Enterprise Applications > IdentityMinder > Manage Modules > policyserver.rar > IdentityMinder.PolicyServerRA > J2C connection factories > PolicyServerConnection > Custom properties
3. Klicken Sie auf den Wert von FIPSMode und setzen Sie ihn auf "True". Klicken Sie auf OK und dann oben auf der Seite auf Link "speichern".

JBoss: Konfigurieren der IPv6-Unterstützung

Wenn Sie die JBoss-Version von Identity Manager auf einem System installieren, das IPv6 unterstützt, ist eine bestimmte Konfiguration erforderlich.

So konfigurieren Sie IPv6 auf einem JBoss-Anwendungsserver

1. Öffnen Sie die Datei "run_idm.sh", die sich an folgendem Speicherort befindet:

   jboss_installation\bin
2. Ändern Sie *eine* der folgenden Eigenschaften im Eintrag "JAVA_OPTS":
   - Für Umgebungen, die ausschließlich IPv6 verwenden, muss das Kommentarzeichen für folgenden Eintrag entfernt werden:

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
   - Für Umgebungen mit IPv6/IPv4 muss das Kommentarzeichen für den folgenden Eintrag entfernt werden:

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
3. Speichern Sie die Datei.

SPML-Unterstützung für FIPS 140-2

Bei Identity Manager r12 ist der SPML-Server mit FIPS 140-2 kompatibel. Wir empfehlen die Bereitstellung des SPML-Services auf:

- Apache Tomcat Server 4.1.36 oder einer höheren Version von 4.1
- JDK 1.5.11 oder einer höheren Version von JDK 1.5. Beachten Sie, dass Tomcat für den SSL-Modus aktiviert werden muss. Details hierzu finden Sie in Apaches Administratorhandbuch für Tomcat 4 (http://jakarta.apache.org/tomcat/), Abschnitt "SSL Configuration HOW-TO".

Wenn Sie CA Tomcat anstelle von Apache Tomcat verwenden, erfordert Identity Manager r12 diese Alternativlösungen für SPML:

- Wenn Sie JDK 1.4.xx mit CA Tomcat verwenden, muss FIPS 140-2 deaktiviert werden. JDK 1.4.xx ist inkompatibel mit CA Tomcat, da die RSA Jsafe CryptoJ 4.0-Bibliothek, die für die FIPS 140-2-Unterstützung benötigt wird, in JDK1.4 nicht als erster Sicherheits-Provider eingestellt werden kann.

  Um die FIPS 140-2-Unterstützung zu deaktivieren, entfernen Sie die JVM-Markierung "-Dcom.ca.commons.security.fips=false" während des Tomcat-Starts.

  - Wenn Sie Tomcat über die Befehlszeile starten, können Sie die JVM-Markierung in der Datei catalina.bat einschließen. Weitere Details finden Sie in der Batchdatei.
  - Wenn Sie Tomcat als Windows-Dienst starten, entfernen Sie die Markierung wie folgt:

    a. Navigieren Sie im Registrierungs-Editor zu "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CA Tomcat 4.1.29 eTrustIAMWebServer\Parameters"

    b. Fügen Sie einen Wert namens "JVM Option Number n" hinzu, wobei 'n' die nächsthöhere Zahl des vorherigen JVM-Parameters ist. Geben Sie als Wert Folgendes ein:

       Dcom.ca.commons.security.fips=false

    c. Erhöhen Sie unter "DWORD_Wert bearbeiten" den Wert "JVM Option Count" um eins, um den neu hinzugefügten Parameter zu berücksichtigen.

- Wenn Sie JDK 1.5 mit CA Tomcat verwenden, besteht ein Inkompatibilitätsproblem. Lösung für dieses Problem:

    a. Entfernen Sie die zwei Xerces-Bibliotheken (xercesImpl.jar und xmlParserAPIs.jar) manuell aus dem Verzeichnis %TOMCATHOME%\common\endorsed.

    b. Starten Sie Tomcat neu.

Änderung der z/OS Connectors-Architektur

Die Architektur der z/OS Connectors (CA ACF2, CA Top Secret und RACF) wurde aus Gründen der Systemleistung überarbeitet, weshalb jetzt anstelle des CA DSI-Servers unter z/OS der CA LDAP-Server für z/OS verwendet wird.

Bevor Sie versuchen, einen z/OS Connector zu konfigurieren, müssen Sie den CA LDAP-Server für z/OS r12 installieren, den Sie von support.ca.com herunterladen können.

Speicherort des eTrust-Verzeichnisses

Das Schema des Bereitstellungsverzeichnisses ist im eTrust-Verzeichnis installiert. Sie können das eTrust-Verzeichnis vom Installationsdatenträger des Identity Manager installieren.

Fehlerbehebung vor der Deinstallation des eTrust-Verzeichnisses erforderlich

Wenn Sie das eTrust-Verzeichnis von einem Windows-Computer deinstallieren möchten, müssen Sie vor der Deinstallation ein Patch anwenden.

Wenn Sie das Patch nicht anwenden, können während des Deinstallationsverfahrens Lizenzdateien gelöscht werden, die noch für andere CA-Produkte benötigt werden.

Sie können das Patch von der CA Support-Website herunterladen.

So finden Sie das Patch

1. Melden Sie sich unter support.ca.com an.

   Die Seite CA Support-Site wird geöffnet.

2. Klicken Sie in der Liste links auf der Seite auf "Licensing" (Lizenzierung).

3. Klicken Sie auf "License Package 1.8 is Now Available" (Lizenz-Paket 1.8 ist jetzt verfügbar).

   Es wird eine Seite geöffnet, die die Änderungen im Lizenz-Paket beschreibt und einen Link zum Herunterladen enthält.

4. Folgen Sie den Anweisungen zum Herunterladen, und installieren Sie das Windows-Patch.

Kapitel 6: Bekannte Probleme

Dieses Kapitel enthält folgende Themen:

Allgemein

Im Folgenden finden Sie bekannte Probleme in Identity Manager r12.

Identity Manager-EAR wird nicht automatisch mit WebLogic bereitgestellt

Wenn Sie WebLogic 8 oder 9 im Produktionsmodus einsetzen, wird Identity Manager-EAR möglicherweise nicht automatisch bereitgestellt, wenn Sie den Anwendungsserver nach einer Installation oder einem Upgrade zum ersten Mal starten. Wenn dieser Fall eintritt, stellen Sie "IdentityMinder.ear" manuell aus dem Ordner "user_projects\applications" bereit.

Workflows und Gruppenmitglieder als Genehmiger

Wenn ein Workflow-Prozess im Workpoint Designer so eingestellt ist, dass ein bestimmtes Gruppenmitglied der Genehmiger dafür ist, kann ein Workflow-Element für das Ereignis nicht unter Workflow-Kontrolle erstellt werden, und die Aufgabensitzung schlägt möglicherweise fehl.

Die Lösung besteht darin, die Aufgabe mit der Vorlagenmethode unter Workflow-Kontrolle zu stellen (mit der Vorlage SingleStepApproval oder TwoStageApprovalProcess), und Gruppenmitglieder als Genehmiger (oder Teilnehmer-Resolver) zu definieren.

Es müssen möglicherweise neue Workpoint-Eigenschaften festgelegt werden.

Identity Manager enthält eine neue Version von Workpoint. In dieser Version können Sie zusätzliche neue Eigenschaften in GeneralMonitor.properties und workpoint-server.properties konfigurieren. Bitte beachten Sie, dass diese neuen Eigenschaften optional sind und nur sofern notwendig hinzugefügt werden sollten.

Die neuen Workflow-Eigenschaften sind:

- In der Datei GeneralMonitor.properties:
  - #JMX_HTML_ADAPTOR_PORT=9092

    Diese Eigenschaft wurde standardmäßig auskommentiert. Wenn der Wert dieser Eigenschaft auf "True" gesetzt ist, wird eine HTML-Seite mit einem generischen Sun JMX-Adapter aktiviert; dabei handelt es sich um einen ungesicherten Webport, der separat von der Workpoint Management-Konsolenanwendung ist. Wir empfehlen unseren Kunden, diese Eigenschaft auskommentiert oder den Wert auf "False" gesetzt zu lassen und stattdessen die Workpoint Management-Konsole für JMX-Zugriff auf Workpoint zu verwenden.
  - JOB_ERROR_STATE_ON_MAIL_ERROR=false

    Diese Eigenschaft ist nur für Kunden verfügbar, die die Workpoint-E-Mail-Funktion verwenden. Diese Eigenschaft steuert die Fehlerverarbeitung im Mail-Monitor. Wenn Identity Manager-Kunden die E-Mail-Funktion von Workpoint benutzen, kann diese Eigenschaft verfügbar sein.

    Hinweis: JOB_ERROR_STATE_ON_MAIL_ERROR ist standardmäßig auf "True" gesetzt, sofern nicht eingestellt. Es empfiehlt sich u. U., den Wert auf "False" zu setzen, wenn Sie Workflow-E-Mail verwenden und E-Mail-Fehler den Jobstatus nicht beeinflussen sollen.
  - ENABLE_SCRIPT_TASK_GROUPING=false

    Diese Eigenschaft steuert, ob der Skript-Monitor alle gleichzeitigen Skripts gruppieren soll, die von demselben Job ausgeführt werden. Wenn der Wert auf "True" gesetzt ist, werden alle Skripts für einen bestimmten Job demselben Arbeitsthread zugewiesen, in dem Sie gleichzeitig ausgeführt werden. Dies ist hilfreich, um Ausnahmen wegen gleichzeitigen Zugriffs zu vermeiden, wenn sich mehrere Aktivitäten in einem Job befinden, die ein asynchrones Skript zur Automatisierung verwenden und möglicherweise gleichzeitig aktiv sind.

    Probieren Sie diese Eigenschaft aus, wenn Sie benutzerdefinierte Workflow-Skripts verwenden und Ausnahmen wegen gleichzeitigen Zugriffs auftreten.

    Zusätzliche E-Mail- und darauf bezogene Eigenschaften finden sich in der Datei GeneralMonitor.properties.

- In der Datei workpoint-server.properties:
  - server.automated.delay=500

    Diese Eigenschaft steuert die Server-automatisierten Knoten, um zu gewährleisten, dass diese Knoten in der Warteschlange nicht bedient werden, bevor die Datenbanktransaktion, die sie in die Warteschlange gestellt hat, eine Chance hat, bestehen zu bleiben. Dadurch werden Server-automatisierte Knotenfehler wegen Zeitplanungsproblemen vermieden. Diese Eigenschaft wird empfohlen, wenn Server-automatisierte Knoten verwendet werden.

Es können keine Kopien von einem Logical-Attribute-Handler erstellt werden

Wenn Sie in der Benutzerkonsole versuchen, eine Kopie eines Logical-Attribute-Handlers zu erstellen, wird folgende Fehlermeldung angezeigt:

"Dieses Objekt ist nicht verbunden"

Das Erstellen eines neuen Logical-Attribute-Handlers, der nicht auf einem bestehenden Logical-Attribute-Handler basiert, funktioniert ordnungsgemäß.

Verwenden von Gruppenfiltern in Rollenrichtlinien

Wenn Identity Manager einen Benutzerspeicher in einer relationalen Datenbank verwaltet, kann es vorkommen, dass Gruppenfilter in den Mitglieder- und Admin-Richtlinien nicht korrekt funktionieren. Beispiel: Wenn Sie in einer Mitgliederrichtlinie einen Filter festlegen wie "Benutzer, die Mitglied von Gruppen sind, deren Name mit 'A' beginnt", wendet Identity Manager die Richtlinie eventuell fälschlicherweise auf alle Benutzer an, anstatt nur auf Benutzer in Gruppen, die mit dem Buchstaben "A" beginnen.

Um dieses Problem zu vermeiden, müssen Sie sicherstellen, dass die Tabellen "tblGroupMembers" und "tblGroupAdministrators" für das Benutzerobjekt in der Konfigurationsdatei (directory.xml) definiert sind.

Die Definition des Benutzerobjekts in "directory.xml" sollte etwa wie folgt aussehen:

```
<ImsManagedObject name="User" description="My Users" objecttype="USER">
<!-- COMMENT Table -->
    <Table name="tblUsers" primary="true" />
    <Table name="tblUserAddress">
    <Reference childcol="userid" primarycol="id"/>
    </table>

    <Table name="tblUserRoles">
    <Reference childcol="userid" primarycol="id"/>
    </table>

    <Table name="tblUserDelegators">
    <Reference childcol="userid" primarycol="id"/>
    </table>

    <Table name="tblUserPasswordhints">
    <Reference childcol="userid" primarycol="id"/>
    </table>

    <Table name="tblUserIdentityPolicy">
    <Reference childcol="userid" primarycol="id"/>
    </table>

    <Table name="tblOrganizations">
    <Reference childcol="id" primarycol="org"/>
    </table>

    <Table name="tblGroupMemebers">
    <Reference childcol="userid" primarycol="id"/>
    </table>

    <Table name="tblGroupAdmins">
    <Reference childcol="userid" primarycol="id"/>
    </table>
```

Importieren Sie die geänderte Verzeichniskonfigurationsdatei mit Hilfe der Management-Konsole.

Hinweis: Weitere Informationen zur Änderung der Verzeichniskonfigurationsdateien finden Sie im *Konfigurationshandbuch*.

Konfigurieren der Rollen- und Aufgabensuchfenster

Wenn Sie Suchfenster für Rollen und Aufgaben konfigurieren, können Sie die Rollen und Aufgaben, die von der Suche zurückgegeben werden, einschränken, indem Sie die Option "Nur Objekte anzeigen, die die folgenden Regeln erfüllen" verwenden. Attribute, die bei der Konfiguration dieser Option nicht verwendet werden, sollten im Suchfenster nicht als verfügbare Suchfelder angezeigt werden.

Beispiel: Wenn Sie das Suchfenster so konfigurieren, dass nur Rollen angezeigt werden, bei denen das Attribut "Aktiviert" auf "JA" eingestellt ist, dann entfernen Sie das Attribut "Aktiviert" aus der Attributliste, über die der Benutzer Suchkriterien festlegen kann.

Andernfalls werden die vom Benutzer eingegebenen Kriterien ignoriert.

Erstellen einer Identity Manager-Umgebung in Firefox-Browsern

Wenn Sie auf die Management-Konsole über einen Firefox-Browser zugreifen, erfolgt die Erstellung einer Identity Manager-Umgebung eventuell nur langsam und es kann sein, dass sie hängen bleibt. In diesem Fall wird zwar die Umgebungserstellung fortgesetzt, aber das Browserbild wird nicht aktualisiert, sodass Sie nicht sehen können, wann die Erstellung abgeschlossen ist.

Hinweis: Wenn Sie das Browserfenster schließen, fährt Identity Manager mit der Umgebungserstellung fort.

Upgrades

Es bestehen in Identity Manager r12 folgende Probleme bei Upgrades.

MS SQL- und Oracle-Endpunkte nach Upgrade von eTrust Admin 8.1 SP2 nicht mehr verfügbar

Nach einem Upgrade von eTrust Admin 8.1 SP2 auf Identity Manager r12 erfordern alle MS SQL- und Oracle-Endpunkte, die vor dem Upgrade erfasst wurden, eine manuelle Neukonfiguration mit dem Bereitstellungs-Manager, so dass sie JDBC-URLs anstelle von Datenquellennamen (DSNs) verwenden. Der Grund dafür ist der Wechsel von SuperAgent zu Java CS zur Verwaltung von MS SQL- und Oracle-Endpunkten.

Oracle: Ändern Sie die Details im Eigenschaftenfenster für Oracle-Endpunkte.

Beispiel:

```
jdbc:oracle:thin:@oracle_server_host:1521:ORACLE
```

MS SQL: Klicken Sie mit der rechten Maustaste auf den Endpunkt, und wählen Sie "Benutzerdefiniert, Admin-Kennwort ändern". Die URL und die Verbindungsinformationen können an dieser Stelle geändert werden, ohne dass man dazu die übrigen Endpunkdetails sehen müsste.

Beispiel:

```
jdbc:sqlserver://serverHost:1433;instanceName=instance1
```

Hinweis: Sie finden die Migrationsschritte und eine vollständige Liste mit möglichen URL-Syntaxen in Kapitel 4: Datenbank-Connectors im *Connectors-Handbuch*.

UNIX Remote-Agent ist nicht für die Solaris x86 (Intel)-Plattform verfügbar

Im Unix Remote-Agent-Paket fehlen Dateien, die für die Installation oder ein Upgrade des UNIX Remote-Agents auf der Solaris x86 (Intel)-Plattform erforderlich ist.

Z/OS Connector-Architektur geändert

Die Architektur der z/OS Connectors (CA ACF2, CA Top Secret und RACF) wurde aus Gründen der Systemleistung überarbeitet, weshalb jetzt anstelle des CA DSI-Servers unter z/OS der CA LDAP-Server für z/OS verwendet wird.

Bevor Sie versuchen, einen z/OS Connector zu konfigurieren, müssen Sie den CA LDAP-Server für z/OS r12 installieren, den Sie von support.ca.com herunterladen können.

Wenn Sie ein Upgrade auf Identity Manager r12 durchgeführt haben, führen Sie anschließend für jeden in Ihrem System definierten Endpunkt Folgendes durch:

Von der Endpunkt-Aufgabenanzeige

1. Wählen Sie unter Objekttyp zwischen CA ACF2-, CA Top Secret- oder RACF-Endpunkt.
2. Klicken Sie auf die Schaltfläche "Suchen". Klicken Sie mit der rechten Maustaste auf den Endpunkt, und wählen Sie "Eigenschaften". Geben Sie folgende Informationen ein:

   Im Bereich Mainframe-Serverinformationen:

   - **IP- Adresse/Rechnername** gibt die IP-Adresse des von RACF verwalteten Systems an, auf dem der CA LDAP-Server konfiguriert ist und ausgeführt wird.
   - **LDAP-Port** gibt die Portnummer an, die Sie bei der Installation des CA LDAP-Servers für z/OS angegeben haben. Falls Sie den Mainframe-LDAP-Port nicht kennen, schlagen Sie im Abschnitt "Ihren CA LDAP-Server nach z/OS-Konfigurations informationen überprüfen" nach.
   - **LDAP-Suffix** gibt das verwendete Suffix für diesen Endpunkt an. Dieses Kombinationsfeld wird automatisch mit allen gültigen und verfügbaren Suffixen gefüllt, wenn Sie auf die Schaltfläche "Suffixe abrufen" klicken. Die Suffixe können abgerufen werden, sobald gültige Werte für die Felder "Mainframe-IP-Adresse/Rechnername" und "Mainframe-LDAP-Port" eingegeben wurden.

Bericht:

Es bestehen in Identity Manager r12 folgende Probleme bei Berichten.

Berichtseinschränkung

Mehrere Snapshots, die mit derselben Berichtsaufgabe verknüpft sind, dürfen nicht dieselbe Wiederholungszeit verwenden.

Satisfy=All funktioniert in XML-Datei nicht ordnungsgemäß

In einer XML-Datei mit Snapshot-Parametern reagieren die Parameter satisfy=all und satisfy=any beide identisch mit satisfy=any (ähnlich wie ein OR-Operator).

Aktivieren Sie Cookies für die Aufgabe "Meine Berichte anzeigen"

Um Berichte in Identity Manager mit der Aufgabe "Meine Berichte anzeigen" angezeigt zu bekommen, müssen Sie im Browser Cookies von Drittanbietern zulassen.

ExportALL.xml-Umgebungen und Umgebungen ohne Organisationsunterstützung

Wenn Sie eine XML-Datei für Snapshot-Parameter (z. B.: ExportAll.xml) verwenden, die alle Organisationsobjekte und -attribute exportiert, tritt ein Ausnahmefehler auf, wenn die Umgebung über keine Organisationsunterstützung verfügt. Ein Workaround für dieses Problem ist das Auskommentieren der Organisationsobjekte und -attribute in der Datei ExportAll.xml.

Bereitstellung

Das Bereitstellen von Komponentenabkürzungen für folgende Elemente ist wie folgt definiert:

- ACC: CA Access Control Connector
- ADS: Active Directory Services Connector
- DBZ: DB2 Universal Database für z/OS Connector
- DYN: Dynamic Connector
- E2K: Exchange 2000 Connector
- EEM: Embedded Entitlements Manager Connector
- ETC: UNIX ETC
- FND: Oracle Applications Connector
- INS: Installation
- KRB: Kerberos Connector
- LND: Lotus Notes/Domino Connector
- NDS: Novell Directory Services Connector
- N16: Windows NT Remote Agent
- AS4: OS/400 Connector
- PKI: Entrust PKI Connector
- PLS: CA SSO for Advanced Policy Server Connector
- PSA: Password Sync Agent
- RSA: RSA SecurID Connector

- SAP: SAP Connector
- SBL: Siebel Connector
- UPO: Universal Provisioning Connector
- VMS: OpenVMS Connector
- z/OS: CA ACF2, CA Top Secret, RACF Connectors

Allgemein

Es bestehen in Identity Manager r12 folgende Probleme bei der allgemeinen Bereitstellung.

Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen"

Um die Bereitstellung für eine Identity Manager-Umgebung zu aktivieren, importieren Sie eine Konfigurationsdatei namens ProvisioningOnly-RoleDefinitions.xml, die die Rollen und Aufgaben für die Benutzereinrichtung erstellt.

In dieser Datei ist die Standardeinstellung der Kontosynchronisierung für die Aufgabe "Benutzerkennwort zurücksetzen" deaktiviert. (Bevor Sie die Bereitstellung aktivieren, ist die Synchronisierungseinstellung auf "Bei Abschluss der Aufgabe" gesetzt.)

Um durch das Zurücksetzen des Benutzerkennworts eine Kontosynchronisierung auszulösen, stellen Sie die Kontosynchronisierungsoption ein, nachdem Sie die Datei ProvisioningOnly-RoleDefinitions.xml importiert haben, um die Bereitstellung zu aktivieren.

Benutzerkonsole kann einige Endpunkttypen nicht durchsuchen und korrelieren

Die Aufgaben "Durchsuchen" und "Korrelieren" in der Benutzerkonsole finden folgende Endpunkttypen nicht:

- Kerberos
- UNIX NIS
- Entrust PKI
- Siebel
- Universal Database for z/OS
- Benutzerspezifisch entwickelte Endpunkttypen

Um diese Endpunkttypen zu durchsuchen und zu korrelieren, können Sie den Bereitstellungs-Manager verwenden. Anschließend können Sie Routinekontofunktionen in der Benutzerkonsole ausführen, wie etwa das Zuweisen eines Kontos zu einem dieser Endpunkte.

Durchsuchen und Korrelieren funktioniert nur in einer Zeitzone

In der Benutzerkonsole können Sie eine "Durchsuchen und Korrelieren"-Definition planen. Bei diesem Vorgang muss sich der Client-Browser in derselben Zeitzone befinden wie der Server. Wenn zum Beispiel die Clientzeit Dienstag 22 Uhr und die Serverzeit 7 Uhr ist, wird die "Durchsuchen und Korrelieren"-Definition nicht funktionieren.

Bereitstellungsserver Core Dump unter Solaris

Der Bereitstellungsserver unter Solaris erzeugt beim Beenden des Dienstes eine Core-Datei.

Dies hat keine Auswirkungen auf die Funktionen und kann daher ohne Risiko ignoriert werden.

Bereitstellungsverzeichnis-Installationsprogramm erfordert korrekt aufgelösten Hostnamen

Das Installationsprogramm erfordert einen Hostnamen mit einer korrekt konfigurierten Namensauflösung, wenn das Bereitstellungsverzeichnis und der Bereitstellungsserver auf demselben Rechner installiert werden. Die Installation des Bereitstellungsservers wird fehlschlagen oder zu unbeabsichtigten Ergebnissen führen, wenn der Rechner seinen eigenen Rechnernamen nicht in die beabsichtigte IP-Adresse auflösen kann. Es gibt zwei mögliche Szenarien:

- Sie haben unterschiedliche Namensauflösungsergebnisse für FQDN und Hostname. (Sie haben z. B. in einem IPv4/6Netzwerk eine IPv6-Adresse in DNS registriert, dafür haben Sie aber eine IPv4-Adresse für den Hostnamen über NetBios oder eine Hostdatei definiert). Wenn Sie das Bereitstellungsverzeichnis so konfigurieren, dass es nur IPV6 verwendet, und Sie dann den Bereitstellungsserver mit FQDN installieren, wird die Installation fehlschlagen, da das Installationsprogramm bei bestimmten Schritten während der Installation versucht, den Hostnamen statt den FQDN aufzulösen. Ein Workaround für dieses Problem ist, den Hostnamen und seine IPv6-Adresse zur Hostdatei hinzuzufügen. Dabei handelt es sich aber trotzdem noch um eine Fehlkonfiguration.
- Wenn Sie auf einem Rechner ohne DNS- oder einer anderen Namenssuche versuchen, das Bereitstellungsverzeichnis und den Bereitstellungsserver unter Verwendung einer IP-Adresse zu installieren, wird die Installation aus demselben Grund fehlschlagen.

  Hinweis: CA unterstützt keine Installation über eine IP-Adresse.

Bestimmte Domänenkonfigurationen, die mit gleichzeitiger globaler Änderung des Benutzerkennworts durchgeführt werden, können zum Absturz des Bereitstellungsservers führen

Wenn für die Domänenkonfiguration für "Identity Manager-Server/Externe Kennwortrichtlinien verwenden" die Option "Ja" ausgewählt ist und eine Vielzahl simultaner globaler Benutzerkennwortänderungen durchgeführt werden. Dies führt zu einer Verschlechterung der Leistung und eventuell zum Absturz des Bereitstellungsservers.

Solaris ECS-Protokollierung oberhalb der INFO-Ebene kann die Leistung des Bereitstellungsservers verringern

Das Aktivieren der ECS-Protokollierung oberhalb der INFO-Ebene führt dazu, dass Protokolle geschrieben werden, bevor Sie eine Antwort erhalten. Dadurch wird Ihre Anfrage verzögert, während das Protokoll geschrieben wird. Wenn die Leistung Ihres Bereitstellungsservers schlecht ist, während Sie die ECS-Protokollierung verwenden, besteht die Problemumgehung darin, diese abzuschalten.

SPML-Updates schlagen fehl, wenn JIAM falsche Objectclass-Namen angibt

Es kann passieren, dass die JIAM-API in an den Bereitstellungsserver gesendeten Anfragen falsche, gekürzte Objektklassennamen verwendet, weshalb der Bereitstellungsserver die Anfrage ablehnt und die Fehlermeldung "Interner Konsistenzfehler im Bereitstellungsserver" ausgibt. Wenn z. B. ein Update des Objekts "eTSBLDirectory" durchgeführt wird, wird die falsche Objektklasse "eTDirectory" an den Bereitstellungsserver gesendet. Dieses Problem kann behoben werden, indem der SPML-Dienst neu gestartet wird.

Sonderzeichen in globalen Benutzernamen

Der Bereitstellungsmanager ermöglicht Ihnen, globale Benutzernamen zu erstellen, die Sonderzeichen enthalten, wie etwa das Backslash-Zeichen (\). Jedoch unterstützt der Identity Manager-Server keine Namen mit Sonderzeichen.

Wenn Sie im Bereitstellungsmanager einen globalen Benutzer mit Sonderzeichen erstellen, versucht Identity Manager, einen entsprechenden Benutzer im Identity Manager-Benutzerspeicher zu erstellen. Es treten Fehler auf und die Aufgabe "Benutzer erstellen" im Identity Manager-Benutzerspeicher schlägt fehl.

Es treten auch Fehler auf, wenn Sie versuchen, einen globalen Benutzer mit Sonderzeichen im Bereitstellungsmanager zu löschen.

Bereitstellungsmanager enthält veraltete SAWI/DAWI-Referenzen

Der Bereitstellungsmanager enthält Dialoge mit Steuerelementen für SAWI- und DAWI-Funktionen, die nicht mehr unterstützt werden. Bitte verwenden Sie die Identity Manager Self-Service-Funktionen anstelle von SAWI oder DAWI.

Fehler "Bereits vorhanden" beim Hinzufügen eines Endpunkts

Wenn Sie einen Endpunkt löschen und mit genau demselben Namen wieder hinzufügen, gibt der Bereitstellungsserver manchmal eine Fehlermeldung aus, dass bereits ein Endpunkt mit dem Namen existiert. Dies kann auftreten, wenn Sie mehrere Connector-Server zum Verwalten des Endpunkts konfiguriert haben. Der Grund für das Fehlschlagen ist ein Problem beim Löschen des Endpunkts, bei dem nicht alle Connector-Server vom Löschen benachrichtigt wurden.

Ein Workaround für dieses Problem ist, alle Connector-Server neu zu starten, die für die Verwaltung des Endpunkts konfiguriert sind.

Java Connector Server (Java CS)

Die folgenden Probleme sind mit dem Java Connector Server in Identity Manager r12 verbunden.

Das Durchsuchen von Java Connector schlägt fehl, wenn die Zeichenfolge " / zur Darstellung von eindeutigen Namen verwendet wird

Es besteht ein ungelöstes Problem in Java CS beim Umgang mit folgender Zeichenfolge:

"/

Sie ist wichtig für den Umgang mit zusammengesetzten Namen, die vom Standard JNDI API verwendet werden, um eindeutige Namen darzustellen, die mehrere Technologien umfassen.

Weitere Informationen über andere Sonderzeichen in eindeutigen Namen, die an Java CS übergeben werden, finden Sie unter "LDAP RFC 2253" auf:

http://ietf.org

und in der JavaDoc für javax.naming.ldap.LdapName

Null-Zeiger-Fehler in Connector Xpress

Wenn Sie versuchen, die Routinginformationen vom Connector Server entweder durch Rechtsklick auf einen Endpunkttyp und Auswahl von "Set Managing CS" oder durch direkte Bearbeitung von CS Configs in Umgebungen mit mehreren Bereitstellungsservern bei Einsatz von Connector Xpress zu ändern, kann Connector Xpress gegebenenfalls einen Null-Zeiger-Fehler anzeigen. Verwenden Sie das csconfig-Tool, wenn Sie erweitertes Connector Server-Routing durchführen möchten.

Neustart des Dienstes Java CS schlägt unter Verwendung von Windows-Diensten fehl

Wenn Sie den Dienst Java CS unter Verwendung von Windows-Diensten neustarten, kann es sein, dass der Dienst Java CS gestartet wird, bevor er vollständig beendet wurde. Dies führt zu einem Fehlschlagen des Neustarts. Wenn dieses Problem auftritt, verwenden Sie bitte die Schaltflächen "Beenden" und "Starten" anstelle der Schaltfläche "Neu starten" in der Windows-Systemsteuerung.

Falsche Fehlermeldung, wenn Sie keine gespeicherte Prozedur wählen

Wenn Sie im Connector Xpress Wizard auf den Bildschirmen zur Tabellenzuordnung aus der Dropdown-Liste "Prozedur wählen" keine gespeicherte Prozedur wählen, wird folgende falsche Fehlermeldung angezeigt:

Bitte geben Sie eine Tabelle an, die zugeordnet werden soll.

Die korrekte Meldung lautet:

Bitte geben Sie eine Prozedur an, die zugeordnet werden soll.

Durchsuchte Container des DYN JNDI-Endpunkts fehlen im Bereitstellungs-Manager

Nach dem Durchführen einer einstufigen Prüfung eines Containers auf neu erhaltene DYN JNDI-Endpunkte zeigt der Inhaltsbereich des Bereitstellungs-Managers eventuell den neu untersuchten Container an, anstelle des Prüfungszählers, der den neu hinzugefügten Datensatz anzeigt. Durch Beenden und erneutes Öffnen des Bereitstellungs-Managers wird die Anzeige des Containers erzwungen.

Gesperrte Attribute der DYN-Kontenvorlage werden im Bereitstellungs-Manager fett dargestellt

Der Bereitstellungs-Manager zeigt das Statusattribut der Sperrung des Kontos fett an, was fälschlicherweise angibt, dass es sich um ein Fähigkeitsattribut handelt.

Bezeichnungen von DYN-Fähigkeitsattributen werden im Bereitstellungs-Manager eventuell abgeschnitten

Beim Erstellen der DYN JDBC- oder DYN JNDI-Endpunkttypen in Connector Xpress angegebene Fähigkeitsattribute können bei der Anzeige im Bereitstellungs-Manager abgeschnitten werden oder ganz fehlen. Dies kann behoben werden, indem am Ende der Bezeichnung ein zusätzliches Zeichen angegeben wird, z. B. "*LabelName a*", wenn der "displayName" in Connector Xpress festgelegt wird. Dies tritt nicht bei Fähigkeitsattributen für Mitgliedschaften auf.

Sie können die vorhandenen Metadaten auch auf eine der folgenden Weisen ändern:

Nach dem Laden des gespeicherten Projekts in Connector Xpress

- Führen Sie den Assistenten aus
- Erweitern Sie die Metadatenstruktur bis zu Klassen -> eTDYNPolicy -> Eigenschaften -> Fähigkeitsattribut -> Metadaten und ändern Sie den Wert für "displayName".

Wenn Sie eines der Verfahren zur Änderung der vorhandenen Metadaten für einen DYN-Endpunkttyp auswählen, müssen Sie sicherstellen, dass Ihr DYN-Endpunkttyp mit den neuen Metadaten aktualisiert wird.

Connectors

Es bestehen in Identity Manager r12 folgende Probleme bei der Bereitstellung von Connectors.

Falsche Ergebnisse bei der Suche in einer Unterstruktur mit ADS Connector

Bei einer Suche in einer Unterstruktur, die mehrere Organisationseinheiten mit einer großen Anzahl an Objekten in den einzelnen Organisationseinheiten enthält, kann es passieren, dass die Suche fälschlicherweise keine Objekte zurückgibt. Wenn die Suche z. B. auf einen Grenzwert von 500 festgelegt wird und die Anzahl der Objekte in den einzelnen Organisationseinheiten diese Größe überschreitet, werden keine Ergebnisse zurückgegeben. Auch wenn der Suchfilter den Grenzwert für die Suche auf einen Wert unter 500 beschränkt, kann es immer noch vorkommen, dass fälschlicherweise keine Objekte zurückgegeben werden. Dieses Problem kann umgangen werden, indem der Grenzwert für die Suche erhöht wird.

Vermeiden Sie ADS-Ablauftermine nach 2038

Wenn Sie das Ablaufdatum für ein ADS-Konto auf ein Datum nach 2038 einstellen, führt dies zum Absturz des Bereitstellungs-Managers.

EEM Connector wird von IE7 nicht unterstützt

Der EEM-Connector wird nicht unterstützt, wenn der C++ Connector Server (CCS) für den betreffenden EEM-Connector auf einem Computer mit IE7 installiert ist.

Hinweis: In der Produktdokumentation von Identity Manager r12 bezieht sich Embedded Entitlements Manager (EEM) auf den Embedded Identity and Access Manager (EIAM)-Connector.

Anzeigen von EEM-Kontenvorlagen mit Bereitstellungs-Manager

Es kann passieren, dass der Bereitstellungs-Manager nicht mehr antwortet, wenn EEM-Kontenvorlagen angezeigt werden.

Dies kann behoben werden, indem der Bereitstellungs-Manager beendet und neu gestartet wird.

Neustart des Bereitstellungs-Managers zum Erfassen eines neuen EEM-Endpunkts

Nachdem ein Hostname während einer Erfassung gesetzt wurde, muss der Bereitstellungs-Manager zur Erfassung eines anderen Endpunkts geschlossen und erneut geöffnet werden. Dies gilt auch, wenn der Vorgang abgebrochen wurde.

Benutzerattribute aus EEM-Kontenvorlage können weder ausgewählt noch geändert werden

Wenn Sie Kontenvorlagen für einen EEM-Endpunkt erstellen, müssen Sie nach der Auswahl des Endpunkts auf die Registerkarte "Anwendungseigenschaften" klicken und dann auf "OK", um den Erstellungsvorgang der Kontenvorlage abzuschließen.

Erfassen von DB2 z/OS-Endpunkt führt zum Absturz von CCS

Die DB2 UDB und DB2 z/OS Connectors dürfen keine Anfragen an denselben C++ Connector Server (CCS) weiterleiten.

Das Problem kann umgangen werden, indem ein zweiter CCS auf einem separaten Computer installiert wird, damit die DB2 UDB und DB2 z/OS Connectors jeweils auf ihrem eigenen C++ Connector Server gehostet werden.

Unbeaufsichtigter Upgrade von ETC UNIX Remote Agent wird nicht unterstützt

Unbeaufsichtigte Upgrades eines ETC UNIX Remote Agent von eTrust Admin r8.1 SP2 auf Identity Manager r12 werden nicht unterstützt. Sie müssen einen beaufsichtigten Upgrade durchführen.

ETC Remote-Agent schlägt unter Linux OS auf einem S390 fehl

Der Versuch, den ETC Remote-Agenten unter einem Linux-Betriebssystem zu installieren, das auf einem S390-Host ausgeführt wird, schlägt mit folgender Fehlermeldung fehl:

"linux098:/home/marty/LinuxS390 # ./IdentityManager.LinuxS390.sh lsm.exe: error while loading shared libraries: libncurses.so.4: cannot open shared object file: No such file or directory."

Ein Workaround dafür ist, eine Version 4 von ncurses für das Betriebssystem zu finden und zu installieren.

Das Ausführen des Befehls "Cafthost" verursacht einen Fehler für HP-UX UNIX

Wenn Sie den folgenden Befehl ausführen, wird möglicherweise die Fehlermeldung "Bus error (Core Dump)" angezeigt:

```
cafthost -a <host_name>
```

Um Hosts hinzuzufügen, müssen Sie die Konfigurationsdatei "cafthost.cfg" manuell mit einem Texteditor im Verzeichnis "cat /etc/catngcampath" ändern und pro Zeile einen Host angeben.

Bei der Deinstallation von ETC Remote Agent können verwaiste Dateien zurückbleiben

Wenn der ETC Remote Agent von r8.1SP2 auf r12 aktualisiert wird, kann es passieren, dass einige Dateien nicht gelöscht werden. Sofern diese Dateien nicht von anderen installierten Paketen verwendet werden, können Sie gelöscht werden:

- /usr/bin/uxsautil
- `cat /etc/catngdmopath.tng`/bin/uxsautil
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/etc/ExitSetup.ini
- `cat /etc/catngdmopath.tng`/scripts/caftexec
- `cat /etc/catngdmopath.tng`/scripts/caftexec.cfg
- `cat /etc/catngdmopath.tng`/setup.gif

Das Löschen von VMS-Kontenberechtigungen mit SPML schlägt fehl

Es ist nicht möglich, einen Wert des Attributs "accountRights" für ein VMS-Konto mit Hilfe von SPML zu löschen. Der SPML-Client gibt eine Erfolgsmeldung zurück, das Konto wird jedoch nicht aktualisiert.

Dieses Problem kann umgangen werden, indem solche Änderungen mit dem Bereitstellungs-Manager durchgeführt werden.

Für OpenVMS-Konten kann kein sekundäres Kennwort festgelegt werden

Das OpenVMS Remote Agent-Hilfsprogramm "vmsautil" erzwingt nicht die Semantik des PRIMÄREN/SEKUNDÄREN OpenVMS-Kennworts für Benutzerkonten. Wenn Sie versuchen, ein sekundäres Kennwort festzulegen, wenn kein primäres Kennwort festgelegt wurde, schlägt dies fehl, und die Fehlermeldung lautet "Kennwort zu kurz".

Das Problem kann umgangen werden, indem das primäre Kennwort immer zurückgesetzt wird, wenn versucht wird, ein sekundäres Kennwort für ein Konto festzulegen.

Bei CAM/CAFT für OpenVMS fehlt eine Anweisung

In der Datei ETRUST_ADMIN_OPENVMS_INSTALLATION.TXT fehlen Informationen darüber, wie CAMCAFT.EXE auf einem OpenVMS-System konfiguriert wird. Der symbolische Namen von CAFTHOST muss vor der Installation von CAM/CAFT definiert werden. Um CAFTHOST zu definieren, fügen Sie folgenden Befehl in die Datei LOGIN.COM ein:

```
CAFTHOST :==$CAPOLY$BIN:CAFTHOST.EXE
```

Melden Sie sich dann wieder beim OpenVMS-System an.

VMS-Attribut "eTVMSPWDLifeTime" zeigt an, dass keine Synchronisierung durchgeführt wurde

Das Attribut für die maximale Gültigkeitsdauer für Kennwörter (eTVMSPWDLifeTime) wird nach dem Kontosynchronisierungsvorgang als nicht synchronisiert angezeigt, wenn das Kontenvorlageattribut "Verfällt nie" aktiviert ist.

VMS-Kontostatus wird durch SPML fälschlicherweise als "Falsch" ausgegeben

Wenn ein VMS-Konto gesperrt ist, gibt der Bereitstellungs-Manager den Kontostatus richtig als "Aktiv (In eTrust Admin gesperrt)" an. SPML gibt dies jedoch fälschlicherweise nur als gesperrt an

VMS-Kennwortflags können nicht gesetzt werden

Das Attribut "eTVMSPwdFlags" wird beim Hinzufügen oder Ändern eines Kontos nicht korrekt gesetzt, wenn die Anfrage nicht auch einen Wert für "eTVMSAccessFlags" festlegt.

Um dieses Problem zu umgehen, sollte eine Anfrage zum Hinzufügen oder Ändern einen Wert für das Attribut "eTVMSAccessFlags" sowie für das Attribut "eTVMSPwdFlags" enthalten.

VMS-Attribut zum Migrieren des Kennworts zeigt an, dass keine Synchronisierung besteht

Alle VMS-Konten oder Kontenvorlagen, bei denen das Feld "MIGRATEPW" aktiviert ist, zeigen nach einer Synchronisierungsprüfung die eTVMSPwdFlags als nicht synchronisiert an.

VMS-Kontosperrung

Das Sperren eines Kontos auf der Kontoebene mit dem Bereitstellungs-Manager sperrt das Konto erfolgreich, behält auf der Eigenschaftenseite jedoch den Eintrag "Gesperrt" nicht bei, sondern ändert ihn wieder in “Aktiv”, sobald die Änderung angewendet wird. Damit haben Sie ein gesperrtes Konto, auf der Eigenschaftenseite des Kontos wird jedoch als Attribut "Aktiv" angezeigt, was bedeutet, dass Sie das Konto nicht erneut aktivieren können.

Für dieses Problem gibt es für das Konto als solches keine Umgehung. Sie können dies nur umgehen, indem Sie das Konto mit einem globalen Benutzer korrelieren und die Sperrung des Kontos über die Sperrung des globalen Benutzers steuern

VMS-Benutzernamen dürfen keine Unicode-Zeichen enthalten, denen kein Escape-Zeichen vorangestellt ist

Wenn versucht wird, ein VMS-Konto mit einem falschen Namen zu erstellen, kann dies zum Absturz des unter Solaris installierten Bereitstellungsservers führen.

NDS Connector kann keine neuen Container durchsuchen

Bei der ersten Suche werden Container gesucht und hinzugefügt, nachdem ein NDS-Endpunkt erfasst wird. Wenn Sie Container mit lokalen NDS-Tools hinzufügen und dann versuchen, den Endpunkt erneut zu durchsuchen, werden weder der neu hinzugefügte Container noch die untergeordneten Einträge in der Struktur angezeigt.

Sie müssen den Endpunkt auf dem Bereitstellungsserver löschen und ihn dann erneut erfassen und durchsuchen, damit die neuen Container angezeigt werden.

NDS-Connector-Beschreibung ist ein einwertiges Feld

Im NDS-Connector ist die Kontobeschreibung ein einwertiges Feld, im NDS-Endpunkt ist die Kontobeschreibung aber ein mehrwertiges Feld.

Die Umgebungsvariable muss nach dem Upgrade gelöscht oder geändert werden, um Probleme mit dem Endpunkttyp "UPO Connector" zu vermeiden

Während eines Upgrades eines Remote SuperAgents auf r12 C++ Connector Server kann es vorkommen, dass die Umgebungsvariable "ETAHOME" den falschen Installationspfad des CCS enthält, was Probleme mit dem Endpunkttyp des UPO Connector verursacht. Sie müssen die Umgebungsvariable "ETAHOME" nach dem Upgrade manuell löschen oder sie im Hinblick auf den richtigen Installationspfad des CCS anpassen, um den UPO-Endpunkt zu erfassen oder zu verwenden.

Beim Abrufen eines UPO-Endpunkts wird kein Domänenfeld überprüft

Ein UPO-Endpunkt mit einem falsch spezifizierten Wert im Domänenattribut wird erfolgreich erfasst, während des Durchsuchens wird aber die Fehlermeldung "Connector Server-Suche fehlgeschlagen: Zugriff nicht ausreichend" ausgelöst.

Dies kann behoben werden, indem Sie im Bereitstellungs-Manager mit der rechten Maustaste auf den Endpunkt klicken und "Benutzerdefiniert -> Anmeldeinformationen aktualisieren..." auswählen und dann den für die Domäne passenden Wert angeben.

Das Prüfen der erforderlichen Kernel-Parameter wird erst nach der Aktualisierung von eTrust Common Services auf Enterprise Common Services unter Solaris durchgeführt

Das Prüfen der erforderlichen Kernel-Parameter wird nicht für Produkte durchgeführt, die eTrust Common Services auf Enterprise Common Services unter Solaris aktualisieren (betrifft eher Solaris 9 als Solaris 10) . Wenn die Kernel-Parameter nicht ausreichend sind wird eine Installation weiter ausgeführt, anstatt mit einer Warnung angehalten. Dies betrifft:

- RSA Remote Agent unter Solaris
- IMPS unter Solaris
- IMPS SDK

So können Sie dieses Problem umgehen:

Ausführen

```
'<product installer dir>/solaris/ecs-installation/eCSinstall.sh'
```

Sofern der Kernel die Parameteranforderungen nicht erfüllt, wird eine Meldung ausgegeben. Wenn die Kernel-Parameter ausreichen, wird das Installationsprogramm gestartet

KRB-Konten können nicht dupliziert werden

Wenn Sie im Bereitstellungsmanager versuchen, ein Kerberos-Konto zu duplizieren, kann dies zum Fehler "eTKRBFullNameCorrelate kann nicht in der Attributregistrierung gefunden werden! (...) - Rückgabecode: 111" führen. Fügen Sie zur Lösung dieses Problems ein neues Konto hinzu, anstatt ein Konto zu duplizieren.

Fehler beim Angeben eines ungültigen REALM bei der Erfassung eines KRB-Endpunkts

Wenn Sie versuchen, einen KRB-Endpunkt zu erfassen und einen ungültigen Wert für den REALM (Bereich) angeben, wird ein Null-Zeiger-Fehler ausgegeben.

z/OS-Sicherheitsendpunkt führt zum Absturz des Solaris Bereitstellungsservers

Wenn der Endpunkt keine Verbindung zum CA LDAP-Server für z/OS r12 herstellen kann, stürzt der Bereitstellungsserver ab.

Um dieses Problem zu umgehen, müssen Sie sicherstellen, dass der Endpunkt mit gültigen Verbindungsinformationen konfiguriert ist

z/OS-Synchronisierung verwendet LDS-Endpunkt

Der LDS-Synchronisierungsagent ist nicht auf der Identity Manager r12-Produkt-DVD enthalten. Kontaktieren Sie den Support, wenn Sie diesen Agenten benötigen.

E2K-Fehlermeldung beim Verwalten von Rechten für Postfächer mit Exchange 2007

Postfachberechtigungen können nicht mit Exchange 2007 verwaltet werden. Sie erhalten die Fehlermeldung "CAFT Message: Access Denied - or command failed to execute" (CAFT-Meldung: Zugriff verweigert – oder Befehl konnte nicht ausgeführt werden).

E2K CAFT-Fehler beim Verwalten von Postfachberechtigungen

Möglicherweise wird bei der Verwaltung von Postfachrechten auch dann die Fehlermeldung “CAFT Message : Access denied - or command failed to execute” (CAFT-Meldung: Zugriff verweigert – oder Befehl konnte nicht ausgeführt werden) zurückgegeben, wenn Ihr Exchange Remote Agent korrekt konfiguriert ist.

Dies kann vorkommen, wenn die Liste der Postfachrechte mehrere Berechtigungen für dasselbe Objekt enthält. Normalerweise passiert dies, wenn die verwalteten Austauschobjekte Rechte übergeordneter Objekte übernehmen.

Für E2K werden nicht mehrere primäre E-Mail-Adressen zugelassen

Es ist mit dem Bereitstellungs-Manager möglich, eine neue E-Mail-Adresse zu einer bestehenden Liste mit E-Mail-Adressen hinzuzufügen und die neue Adresse als primäre E-Mail-Adresse festzulegen. Eine vorhandene primäre E-Mail-Adresse wird jedoch nicht zurückgestuft. Dies kann dazu führen, dass ein Konto mehrere primäre E-Mail-Adressen besitzt, was im nativen System nicht zulässig ist. Dies lässt sich vermeiden, indem die vorhandene primäre E-Mail-Adresse zuerst zurückgestuft wird, bevor die neue primäre E-Mail-Adresse hinzugefügt wird

Langer PKI-Pfad zur INI-Datei kann einen Neustart des Bereitstellungsservers auslösen

UNC-Pfade mit mehr als 77 Zeichen lösen einen Neustart des Betriebssystems aus. Um dies zu umgehen, verwenden Sie keine langen Pfade.

PKI-Konten erscheinen doppelt

Der PKI-Connector unterstützt keine hierarchischen Entrust PKI-Endpunkte und speichert alle Konten in einer einfachen Liste. Daher erscheint ein eindeutiges Entrust PKI-Konto für den PKI-Connector doppelt.

Das Fenster der PKI-Gruppeneigenschaften wird nicht korrekt angezeigt

Wenn Sie versuchen, ein PKI-Gruppeneigenschaftenfenster im Bereitstellungs-Manager zu öffnen, wird die Fehlermeldung "Unable to display the requested property sheet" (Fehler bei der Anzeige des angeforderten Eigenschaftenfensters) angezeigt.

E-Mail-Benachrichtigungswarnung beim Erstellen von PKI-Konten

Wenn Sie einen PKI-Endpunkt mit Hilfe eines Proxy-Profils erfassen und die E-Mail-Benachrichtigung eingeschaltet ist, dann können Sie ein neues PKI-Konto nur erstellen, wenn Sie die Option "Profil erstellen" angeben.

So umgehen Sie das Problem:

- Erfassen Sie den Endpunkt ohne das Proxy-Profil.
- Schalten Sie die E-Mail-Benachrichtigungen ab, wenn Sie den Endpunkt erfassen, und prüfen Sie die Referenznummer des Endpunkts manuell

SAP-vertragliche Benutzertypen zuweisen

enn ein vertraglicher Benutzertyp einem Benutzer auf der Registerkarte "Lizenzdaten" zugewiesen wird, kann die Änderung nur auf das Master-System und auf kein Tochter-System angewendet werden.

Es ist möglich, die vertraglichen Lizenztypen für die Untersysteme von vornherein zu ändern.

Pflichtfelder im SAP-Attribut "Vertraglicher Benutzertyp"

Der vertragliche Benutzertyp, der in der Registerkarte "Lizenzdaten" des Kontos angegeben ist, darf keine anderen Pflichtfelder enthalten als das Feld LIC_TYPE. Wenn Sie z. B. den Namen von einem SAP R3-System (SYSID) angeben sollen, um einen vertraglichen Benutzertyp zu verwenden, wird die Zuweisung fehlschlagen, und Sie erhalten eine Fehlermeldung, dass ein Wert für den Namen des SAP R3-Systems fehlt.

C++ Connector Server stürzt während einer Anfrage an den PLS Connector möglicherweise ab

Wenn Sie feststellen, dass Ihr CCS bei einer Anfrage an einen PLS Connector abstürzt, prüfen Sie Ihre Richtlinienserverinstallation, da diese das Problem verursachen kann. Als Symptom werden Sie feststellen, dass Ihre Anfragen beim Richtlinienserver deutlich langsamer verarbeitet werden, weil der Access Control-Dienst ständig neu gestartet wird.

SBL-Kontosperrung

Wenn Sie ein SBL-Konto oder eine SBL-Kontenvorlage ändern und die Änderungen mit einem Konto synchronisieren, dürfen Sie zusammen mit den Änderungen kein "eTSuspended" senden, da dies dazu führt, dass die anderen Attributänderungen ignoriert werden.

Um dies zu umgehen, müssen Sie die Änderungen auf zwei separate Anfragen aufteilen, von denen eine die eTSuspended-Änderungen enthält und die andere die Änderungen der Werte der anderen Attribute.

Fehlerhafte Meldung bei JIAM RSA-Kontosynchronisierungsprüfung

Wenn Sie eine Kontosynchronisierungsprüfung für ein RSA-Konto mit JIAM durchführen und das Konto im Endpunkt fehlt, meldet der Connector Server fälschlicherweise ein Fehlschlagen und die Meldung "Connector Server-Lesefehler: Sd_GetSerialByLogin-Fehler - Ungültiger Benutzer" anstelle eines Erfolgs und der Meldung "Konto fehlt im Endpunkt". Prüfen Sie, ob die Kontosynchronisierung im Bereitstellungsmanager ordnungsgemäß funktioniert.

Das Entfernen mehrerer Gruppen von einem OS/400-Benutzer blockiert den Bereitstellungs-Manager

Wenn mehrere Gruppen von einem Benutzer in einem einzelnen Durchlauf entfernt werden und mehrere Gruppen mit "#" beginnen, kann dies dazu führen, dass der Bereitstellungs-Manager nicht mehr antwortet.

Um dies zu umgehen, müssen Sie die Gruppen nacheinander entfernen.

Für ein OS/400-Konto darf die primäre Gruppe nicht entfernt werden

Die OS/400-Gruppenmitgliedschaft kann geändert werden, indem entweder das Konto geändert wird, das Gruppenmitglied ist, oder indem die Mitgliedschaft der Gruppe geändert wird. Wenn die Mitgliedschaft einer Gruppe geändert wird, können Konten nicht entfernt werden, wenn es sich bei Ihrer Gruppenmitgliedschaft um eine primäre Gruppenmitgliedschaft handelt.

Um dies zu umgehen, müssen Sie das Konto ändern und die primäre Gruppenmitgliedschaft entfernen.

Für den FND Connector muss in der Zuständigkeitsliste ein "Von"- und ein "Bis"-Datum angegeben sein

Der FND Connector muss in der Zuständigkeitsliste sowohl ein "Von"- als auch ein "Bis"-Datum enthalten, andernfalls wird die Zuständigkeitsliste instabil und kann nicht wiederhergestellt werden.

Um dieses Problem zu umgehen, müssen Sie in der Liste der Zuständigkeiten immer ein "Von"- und ein "Bis"-Datum angeben, beim Erstellen oder Ändern des FND-Kontos oder der Kontenvorlage (indem Sie z. B. weit in der Zukunft liegende Datumsangeben verwenden, anstatt für "Von" und "Bis" keine Angaben zu machen).

Cafthost-Definition unter VISTA funktioniert nicht

Wenn Sie den N16 Remote Agent auf einem VISTA- oder VISTA SP1-Endpunkt installiert haben und versuchen, den Server über "Alle Programme -> CA - > Identity Manager -> Cafthost-Definition" zu verwalten, und dann versuchen, den entsprechenden VISTA-Computer als Endpunkt zu erfassen, erhalten Sie die Fehlermeldung 'Zugriff verweigert'.

Um dies zu umgehen, müssen Sie eine Eingabeaufforderung öffnen und den Endpunkt mit dem folgenden Befehl erfassen.

```
cafthost -a <hostname/IP>
```

Verwenden Sie absolute Pfadangaben, um auf Speicherorte benutzerdefinierter Kennungen von LND-Konten und auf Zertifikatkennungen der Organisationseinheit zuzugreifen

Die Verwendung von UNC-Pfaden beim Zugriff auf Speicherorte benutzerdefinierter Kennungen für Konten und Zertifikatkennungen von Organisationseinheiten funktioniert mit freigegebenen Ordnern und relativen Pfadangaben nicht immer. Es empfiehlt sich die Verwendung absoluter Pfadangaben (mit Laufwerksbuchstabe).

LND-Suchanfrage in SPML gibt keine Ergebnisse zurück

Die Durchführung einer Suchanfrage in SPML oder über den SPML-Server für ein Konto gibt keine Ergebnisse zurück, wenn neben "lastName" und "homeServer" weitere Attribute verwendet werden

Das Korrelieren von LND-Konten und globalen Benutzern, die über SPML erstellt wurden, funktioniert nicht

Im Bereitstellungs-Manager funktioniert das Korrelieren von Konten und globalen Benutzern, die über SPML erstellt wurden, derzeit nicht.

Vermeiden Sie, in LND-Kontonamen japanische Zeichen zu verwenden.

Das Ändern von ID/Kennwort funktioniert zurzeit nicht für Konten, deren Namen japanische Zeichen enthalten. Dieses Problem lösen Sie, indem Sie in der Kontokennungsdatei englische Zeichen verwenden.

LND-Konten können nicht mit "Benutzereindeutige OE" erstellt werden

Konten können nicht mit "Benutzereindeutige OE" erstellt werden. Das daraus resultierende Konto kann nicht gesucht werden und es ist kein Zugriff mit dem Bereitstellungs-Manager möglich.

Das Attribut für den Kurznamen eines LND-Kontos darf maximal 85 japanische Zeichen enthalten

Wenn Sie im Attribut für den Kurznamen des Kontos mehr als 85 japanische Zeichen verwenden, kann dies den Domino-Server zum Absturz bringen. Dieses Problem tritt nur auf, wenn der Kontoname auch japanische Zeichen enthält.

Der Bereitstellungs-Manager zeigt keine Gruppenmitgliedschaften des LND-Kontos an, wenn japanische Zeichen enthalten sind

Im Bereitstellungs-Manager werden für Konten, die in Organisationen und Organisationseinheiten erstellt wurden und japanische Zeichen enthalten, auf der Registerkarte "Mitglied von" keine Gruppenmitgliedschaften angezeigt.

Auf LND-Konto- und Zertifizierer-IDs, die japanische Zeichen enthalten, ist kein Zugriff über den LND JCS Connector möglich

Auf Konto- und Zertifizierer-IDs, die japanische Zeichen enthalten, ist kein Zugriff über den LND JCS Connector möglich. Alle Funktionen, die auf diese ID-Dateien zugreifen müssen, werden in dieser Version fehlerhaft ausgeführt.

Japanische Zeichen in DN-Pfaden von LND-Objekten können beim Durchsuchen des Verzeichnisses Probleme verursachen

Einige japanische Zeichen in DN-Objekt-Pfaden sorgen dafür, dass sich der Bereitstellungsserver bei der Verzeichnissuche aufhängt. Beispiele: Japanische Zeichen mit Unicode 0x80fd, 0x4e88 und 0x5642.

LND Connector kann kein Umbenennen oder Verschieben durchsuchter LND-Konten in der Hierarchie durchführen

Diese Version des LND Connectors kann für durchsuchte LND-Konten die benutzerdefinierten Aktionen zum Umbenennen oder Verschieben in der Hierarchie nicht durchführen. Die Attributfelder sind für diese Aktionen deaktiviert.

Hierfür gibt es keine Lösungsmöglichkeit.

LND-Konto und die zugehörige Mail-Datei können nicht unter Verwendung der benutzerdefinierten Aktion gelöscht werden

Das Löschen eines Kontos und der Mail-Datei des Kontos mit der Aktion "benutzerdefiniert" schlägt fehl.

Der Bereitstellungs-Manager gibt keine Fehlermeldung aus, aber eine Untersuchung der Endpunkte zeigt, dass sowohl das Konto als auch die zugehörige Mail-Datei noch vorhanden sind. Für die Verwendung des Bereitstellungs-Managers gibt es in diesem Punkt keine Problemlösung.

Bei der Registrierung werden keine Mailfehler für LND-Konten erzeugt

Das Fenster des Bereitstellungs-Managers zur Kontoerstellung enthält auf der Registerkartenseite "Profil" ein Kontrollkästchen "Replikate erstellen".

Wenn ein Domino-Endpunkt verwaltet wird, der sich in einer Cluster-Umgebung befindet, und wenn das Kontrollkästchen "Replikate erstellen" aktiviert ist, sollte in der Cluster-Umgebung ein Replikat des Kontos zusammen mit der zugehörigen Mail-Datei erstellt werden. Das Erstellen von replizierten Mail-Dateien wird in dieser Version während der Registrierung nicht behandelt.

Kapitel 7: Dokumentation

Die Dateinamen der Identity Manager r12-Handbücher sind:

Handbuchname	Dateiname
Versionshinweise	im_release_enu.pdf
Implementierungshandbuch	im_impl_enu.pdf
Installationshandbuch für WebLogic	im_install_weblogic_enu.pdf
Installationshandbuch für WebSphere	im_install_websphere_enu.pdf
Installationshandbuch für JBoss	im_install_jboss_enu.pdf
Konfigurationshandbuch	im_config_enu.pdf
High Availability-Handbuch	im_high_avail_enu.pdf
Administrationshandbuch	im_admin_enu.pdf
Programmierhandbuch für Java	im_dev_enu.pdf
Programmierhandbuch für die Bereitstellung	im_dev_provisioning_enu.pdf
Bereitstellungshandbuch	im_provisioning_enu.pdf
Connectors-Handbuch	im_connectors_enu.pdf
Handbuch für Connector Xpress	im_connector_xpress_enu.pdf
Implementierungshandbuch für Java Connector Server	im_jcs_impl_enu.pdf
Programmierhandbuch für Java Connector Server	im_jcsProg_Enu.pdf
iRecorder-Integrationshandbuch	audit_im_irec_ref_enu.pdf
Glossar	im_glossary.pdf
Bookshelf	im_bookshelf_enu.zip

Die Identity Manager r12-Handbücher stehen unter folgender Location zum Herunterladen zur Verfügung:

- CA Support-Webseite:

Um PDF-Dateien anzeigen zu können, müssen Sie Adobe Reader 7 oder höher von der Adobe-Website herunterladen, falls dieser noch nicht auf Ihrem Computer installiert ist.

Hinweis: Wenn Sie den Bookshelf auf einem Remote-System installieren, werden die besten Ergebnisse erzielt, wenn auf den Bookshelf über einen Webserver zugegriffen werden kann.

Dieses Kapitel enthält folgende Themen:

Bookshelf

Der Bookshelf ermöglicht den Zugriff auf die gesamte Dokumentation von Identity Manager über eine einzige Oberfläche. Er bietet Folgendes:

- Erweiterbare Inhaltsangabe für alle Handbücher im HTML-Format
- Volltextsuche über alle Handbücher mit bewerteten Suchergebnissen und im Inhalt hervorgehobenen Suchbegriffen
- Klickelemente ("Brotkrümel"), die zu übergeordneten Themen führen
- Ein einziger HTML-Index für Themen in allen Handbüchern
- Links auf PDF-Versionen der Handbücher zum Drucken

Verwenden des Bookshelfs

1. Laden Sie den Bookshelf von der Support-Website von CA herunter.
2. Entpacken Sie den Inhalt der Zip-Datei.
3. Zeigen Sie den Bookshelf wie folgt an:
   - Wenn sich der Bookshelf auf dem lokalen System befindet, und Sie Internet Explorer verwenden, öffnen Sie die Datei Bookshelf.hta.
   - Wenn Sich der Bookshelf auf einem Remote-System befindet, oder wenn Sie Mozilla Firefox verwenden, öffnen Sie die Datei Bookshelf.html.

     Hinweis: Um eine bessere Leistung zu erhalten, sollten Sie, wenn Sie den Bookshelf auf einem Remote-System installieren, den Zugriff auf den Bookshelf über einen Webserver zulassen.

Für den Bookshelf ist Internet Explorer 6 oder 7 oder Mozilla Firefox 2 erforderlich. Für die Links auf PDF-Handbücher ist Adobe Reader 7 oder 8 erforderlich. Sie können Adobe Reader unter www.adobe.com herunterladen.

Hinweis: Der CA SiteMinder Bookshelf wurde auf der Support-Website von CA für r12 und r6.0 SP5 in dem Bookshelf-Format für Identity Manager veröffentlicht.

Verbesserungen der Online-Hilfe

Die Online-Hilfe der Benutzerkonsole und der Management-Konsole bieten jetzt die folgenden Funktionen:

"Brotkrümel"-Navigation

Angabe der Position innerhalb der Hierarchie des Hilfesystem für eine einfache Navigation. Die "Brotkrümel" befinden Sich oben auf der Hilfeseite.

Hervorgehobene Suchbegriffe

Kennzeichnet den Kontext der Suche im Ergebnis durch eine gelbe Hervorhebung.

Navigationsschaltflächen

Leichtere Navigation durch Schaltflächen mit Vorwärts- und Rückwärtspfeilen. Die "Brotkrümel" befinden Sich oben auf der Hilfeseite.

Änderung der Marke von eTrust auf CA

Die Marke einige CA-Sicherheitsprodukte befindet sich derzeit im Übergang von “eTrust” zu “CA". Während dieses Übergangs wird in der Dokumentation möglicherweise sowohl auf eTrust-Produkte als auch auf CA-Produkte verwiesen. eTrust Directory wird in der nächsten Version den Markennamen CA Directory tragen. Jede Erwähnung eines eTrust-Produkts in der Dokumentation entspricht demselben Produkt mit dem neuen Markennamen CA.

Änderungen der Terminologie für die Bereitstellung

Kunden mit eTrust Admin stellen möglicherweise fest, dass sich einige Begriffe geändert haben, seit eTrust Admin Teil von CA Identity Manager ist. Die folgende Tabelle zeigt diese Änderungen.

eTrust Admin-Begriff	Neuer Begriff in Identity Manager
eTrust Admin-Server	Bereitstellungsserver
eTrust Admin-Manager	Bereitstellungs-Manager
Verzeichnis	Endpunkt, Endpunkte
Namespace	Endpunkttyp
Richtlinie oder Bereitstellungsrichtlinie	Kontenvorlage
Rollen	Bereitstellungsrollen
Distributed SuperAgent Framework	Connector Server Framework
SuperAgent	C++ Connector Server
Option	Connector
Verwaltungsverzeichnis oder Verwaltungs-Repository	Bereitstellungsverzeichnis
Identity Manager-Unternehmensverzeichnis	Identity Manager-Benutzerspeicher
Corporate User	Innenadministrator

Neuer Name für Embedded IAM (EIAM) Connector

In der Produktdokumentation von CA r12 bezieht sich Embedded Entitlements Manager (EEM) auf den Embedded Identity and Access Manager (EIAM)-Connector

Programmierdokumentation

Zur Dokumentation von Identity Manager r12 gehören zwei Programmierhandbücher.

Programmierhandbuch für Java

Dieses früher als Identity Manager Entwicklerhandbuch bezeichnete Handbuch enthält Informationen zur Verwendung der Java-API von Identity Manager. In die HTML-Version sind Javadoc-Seiten integriert. Sie enthält Hyperlinks, die auf wichtige Informationen verweisen.

Programmierhandbuch für die Bereitstellung

Dieses früher als eTrust Admin SDK Entwicklerhandbuch bezeichnete Handbuch enthält Informationen zum Identity Manager Provisioning Server SDK. Entwickler müssen C++-Programmierkenntnisse besitzen.